

10 JUN 2005

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004年7月1日 (01.07.2004)

PCT

(10) 国際公開番号
WO 2004/055685 A1

- (51) 国際特許分類⁷: G06F 15/00, 12/00, 12/14
 (21) 国際出願番号: PCT/JP2003/016130
 (22) 国際出願日: 2003年12月16日 (16.12.2003)
 (25) 国際出願の言語: 日本語
 (26) 国際公開の言語: 日本語
 (30) 優先権データ:
 特願 2002-366489
 2002年12月18日 (18.12.2002) JP
 (71) 出願人(米国を除く全ての指定国について): インター
 ナショナル・ビジネス・マシーンズ・コーポレー

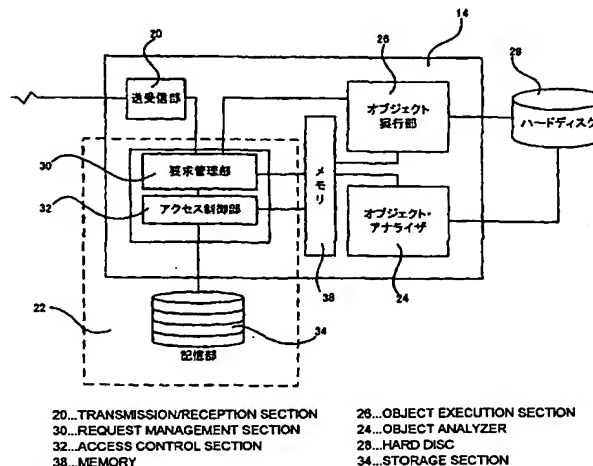
ション (INTERNATIONAL BUSINESS MACHINES
 CORPORATION) [US/US]; 10504 ニューヨーク州
 アーモンク ニューオーチャードロード NY (US).

- (72) 発明者; および
 (75) 発明者/出願人(米国についてのみ): 立堀 道昭 (TAT-
 SUBORI, Michiaki) [JP/JP]; 〒242-8502 神奈川県 大和
 市 下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基
 礎研究所内 Kanagawa (JP). 高瀬 俊郎 (TAKASE, Toshi-
 roh) [JP/JP]; 〒242-8502 神奈川県 大和市 下鶴間1623番
 地14 日本アイ・ビー・エム株式会社 東京基礎研究所内 Kana-
 gawa (JP). 中村 祐一 (NAKAMURA, Yuhichi) [JP/JP]; 〒
 242-8502 神奈川県 大和市 下鶴間1623番地14 日本アイ・
 ビー・エム株式会社 東京基礎研究所内 Kanagawa (JP).

[続葉有]

(54) Title: WEB SERVICE PROVIDING SYSTEM, SERVER DEVICE FOR THE SAME, CONTROL METHOD FOR CON-
 TROLLING COMPUTER SYSTEM AS SERVER DEVICE FOR WEB SERVICE PROVIDING SYSTEM, PROGRAM FOR EX-
 ECUTING THE CONTROL METHOD, AND RECORDING MEDIUM

(54) 発明の名称: Webサービス提供システム、そのためのサーバ装置、コンピュータ・システムをWebサービス提
 供システムのためのサーバ装置として制御するための制御方法、および該制御方法を実行するためのプログラムお
 よび記録媒体



(57) Abstract: There are provided a Web service providing system, a server device for it, a control method for controlling a computer system as a server device for the Web service providing system, a program for executing the control method, and a recording medium. The Web service providing system includes a server device (14). The server device (14) has an object analyzer (24) for acquiring all the methods which may be called out by a request object and generating an access authority set, object execution means (26) for executing a request object, and a storage section (34) for storing the execution result of a past object. Furthermore, the server device (14) has a cache mechanism (22) for executing access control for the storage section (34) in response to an object call request by using the access authority set.

(57) 要約: Webサービス提供システム、そのためのサーバ装置装置、コンピュータ・システムをWebサービス提供シ
 ステムのためのサーバ装置装置として制御するための制御方法、および該制御方法を実行するためのプログラムお
 よび記録媒体を提供する。 本発明のWebサービス提

[続葉有]



(74) 代理人: 坂口 博, 外(SAKAGUCHI, Hiroshi et al.); 〒242-8502 神奈川県 大和市 下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内 Kanagawa (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

供システムは、サーバ装置装置 14 を含んで構成される。サーバ装置装置 14 は、要求オブジェクトが呼出す可能性のあるメソッドすべてを取得してアクセス権限セットを生成するオブジェクト・アナライザ 24 と、要求オブジェクトを実行するためのオブジェクト実行手段 26 と、過去のオブジェクトの実行結果を格納する記憶部 34 を含んで構成され、かつアクセス権限セットを使用してオブジェクト呼出し要求に応答して記憶部 34 に対するアクセス制御を実行するキャッシュ機構 22 とを含んでいる。

明細書

Webサービス提供システム、そのためのサーバ装置、コンピュータ・システムをWebサービス提供システムのためのサーバ装置として制御するための制御方法、および該制御方法を実行するためのプログラムおよび記

5 録媒体

技術分野

本発明は、効率的なWebサービスの提供に関し、より詳細には、ユーザが過去に閲覧したWebサービスの情報に基づき、高速、かつ高信頼性をもってユーザに対してWebサービスの提供を可能とすると共に、ユーザのアクセス権限の変更およびWebサービス提供者のWebサービスへのアクセス権限変更に対して高い柔軟性を付与することが可能なWebサービス提供システム、そのためのサーバ装置、コンピュータ・システムをWebサービス提供のためのサーバ装置として制御するための制御方法、および該制御
10 方法を実行するためのプログラムおよび記録媒体に関する。

背景技術

単純にWebページを表示させるといったスタティックなコンテンツから、JSP (Java (登録商標) Service Provider) のようなダイナミックなコンテンツにいたるまで、様々なコンテンツに対応したWebサービスのためのキャッシュ機構が知られている。例えばWebサービスを行うためのキャッシュ機構として、WebSphereのDynaキャッシュを挙げることができる。従来知られているキャッシュ機構は、以前に実行した結果を覚えておき、ユーザがWebサービスに再度アクセスする際に、実際にサービス・オブジェクトを実行するのではなく、キャッシュ機構に記憶させておいた過去の
20 の実行結果を返すことで応答性能を向上させている。

- 一方で、Web上でサービスを提供する場合には多くの場合、ユーザに応じてアクセスを制限できるようにすることが好ましい場合もあり、ユーザのアクセス権限に応じてアクセスを制限するためのアクセス制御機構も知られている。より具体的には例えば、銀行のATMサービスを提供するWebサイトを構築する場合、ユーザには、その信用や長期預金額などにより、Gold会員、Silver会員、Bronze会員のクラス分け（以下、アクセス権限として参照する。）を付与して高い付加価値のサービスを用意することができる。この場合、Bronze会員は、一般の顧客であり、クラスがSilver、Goldとグレードが高くなるにつれて、ユーザは、より高い価値のサービスの提供を受ける。上述したWebサービスとしては、通常の預金操作の他、アクセス権限で差別化された株（天気）情報の提供、エンターテイメント情報、不動産情報も考えられる。
- 15 上述したユーザのアクセス権限に応じたWebサービスの提供における上述したアクセス制限機能としては、具体的にはHTTPのBasic Authや、EJBにおけるアクセス権限に基づくメソッド単位のアクセス制御機構を挙げることができる。
- 20 図21には、従来のアクセス制御機構を含むWebサービス提供システムの概略的な処理を示す。図21が従来のアクセス制御機構の処理を示した概略図である。図21に示したWebサービス提供システムのアクセス制御機構は、Webサービスを提供するサーバ装置102に備えられており、ユーザは、コンピュータ、セルラ電話、PDAといったユーザ端末104からサーバ装置102へと、有線ネットワークや、無線ネットワーク、
- 25 またはこれらが混在した複合ネットワークであるネットワーク106を

介してサーバ装置 102 へとアクセスしている。サーバ装置 102 へのアクセス認証は、通常ではユーザ識別を実行するためのコード（以下、ユーザ ID として参照する。）およびパスワードといった公衆鍵と秘密鍵との組み合わせにより行われる。サーバ装置 102 によりユーザ認証
5 がなされると、ユーザにより送られたアプリケーション要求、例えば天気予報の情報の提供を行う Weather というアプリケーションの呼出しを要求するオブジェクト呼出し要求がサーバ装置 102 へと入力される。

アプリケーション Weather は、さらにユーザのアクセス権限に応じて、
10 大まかな天気予報をユーザに提供するためのメソッドである RoughWF()、より多様で高付加価値の情報を提供することができるメソッドである WeatherForecast() などと呼出すことが可能とされている。ユーザには、例えばサービス提供者との契約などに基づき、上述した Gold、Silver、Bronze といったアクセス権限が付与されている。図 21 に示した従来例で
15 は、Silver のアクセス権限を有するユーザが、ユーザ端末 104 からサーバ装置 102 へとアクセスしているのが示されている。ユーザは、Weather getRoughWF() といった Silver のユーザにアクセス権限に対応した実行結果を取得し、実行結果は、ブラウザ・ソフトウェアを使用してユーザへとデータが提供される。

20

また、Gold ユーザは、Weather のアプリケーションにおいてさらに、別の getWeatherForecast() というメソッド呼出しが許可されており、さらにその中で、getDetailedInfo というメソッドを呼出すことが許可されているなど、より高い価値の Web サービスへのアクセスが許可される。図 21 では、Gold のアクセス権限を有するユーザのみがメソッド getDetailedInfo() のデータを取得することができ、Silver のアクセス権限を有す

るユーザは、例えば、getDetailedInfo()のメソッドの実行結果を受け取ることができないことが示されている。

図21に示すように、Webサービス提供に対応するメソッドgetRoughWF()およびgetWeatherForecast()については、GoldまたはSilverのアクセス権限を有するユーザに対してアクセスが許されているものとする。このとき注意しなければならないのは、最初に呼ばれるメソッドへのアクセスが許されている場合でも、そのメソッドの内部でさらに呼出されるメソッドへのアクセスが許されているとは限らないことにある。図21のgetWeatherForecast()は、その例であり、メソッドgetWeatherForecast()の内部で呼ばれているメソッドgetDetailedInfo()は、アクセス権限がSilverであるユーザには、アクセスが許されていない。このため、実行結果を返す場合に、getDetailedInfo()が呼出される場合には、メソッドgetWeatherForecast()の実行結果を、アクセス権限がSilverのユーザに返してはならない。一方、メソッドgetRoughWF()は、その後Silverのアクセス権限を有するユーザによるアクセスが許されていないメソッドが呼ばれていないので、その実行結果をSilverのアクセス権限のユーザに返すことができる。

20 図22は、図21に示した従来のアクセス制御機構における他の不都合を示した図である。図22では図21と同様に、ユーザは、ユーザ端末104からサーバ装置102へとネットワーク106を介してアクセスする。図26では、サーバ装置102が含むアクセス制御機能108が示されており、アクセス制御機能108によりアクセス権限がSilver
25 のユーザが、例えばアクセス権限がGoldのユーザにのみ許可される要求がサーバ装置102に入力された場合には、その要求を実行させないこ

とで、アクセス権限がSilverであるユーザが不正にGoldのアクセス権限を必要とするサービスにアクセスしてしまうことを防止している。

一方で、Silverのアクセス権限を有するユーザは、アクセス権限がSilverのユーザに許可されるWeather getRoughWF ()により与えられる実行結果を取得することができる。アクセス権限がSilverのユーザは、許可されたデータの取得が可能ではあるものの、サーバ装置102は、アクセス制御を要求されたメソッドを呼出すたびに実行させる必要があるので、データをブラウザ・ソフトウェア上に表示させるまで長時間を要するといった時間遅延を生じることになる。このような不都合は、サーバ装置の能力や、処理の複雑さなどに依存するので、ADSL、光通信といったブロードバンド通信が普及し、サーバ装置—ユーザ端末間の通信速度が高くなっても改善されるものではない。

15 上述した従来の不都合を改善するために、サーバ装置102にキャッシュ機構を導入することもできる。図23は、従来のアクセス制御機構に対して、キャッシュ機構を導入したシステムを示す。

図23に示したシステムは、サーバ装置102がキャッシュ機構110を含んで構成されており、ユーザが送信したオブジェクト呼出し要求により呼出されたオブジェクトが実行した実行結果が、キャッシュ機構110に格納される構成とされている。図23に示されるように、サーバ装置102に対してキャッシュ機構110とアクセス制御機構108とを構成させる場合には、ユーザはそれぞれのアクセス権限を有するサービスに対して適正なアクセス権限を行使して実行結果を取得することが可能となる。またユーザにより取得された実行結果は、キャッシュ機

構 1 1 0 に格納されるので、過去に要求したと同一のオブジェクト呼出を要求するユーザは、キャッシュ機構に格納された過去の実行結果を容易に取得することが可能となる。また、キャッシュ機構から送られた実行結果に基づいてその後の処理を容易に実行させることが可能となる。

- 5 しかしながら、従来のアクセス制御を伴うWebサービスに関していえば、後述する理由から、キャッシュ機構を使用しない構成が採用されてきた。

- すなわち、図 2 3 に示されるように、サーバ装置 1 0 2 に対してキャッシュ機構 1 1 0 と、アクセス制御機構 1 0 8 とを同時に使用する場合
10 を考える。キャッシュ機構 1 1 0 が、ユーザのアクセス権限に無関係にユーザのアクセスを許可してしまう場合には、いったんキャッシュ機構に格納された実行結果が、ユーザのアクセス権限に関係なく同一のサービスを要求するユーザに対して提供されてしまうという不都合が生じる。
- 15 このようなアクセス権限に基づかないキャッシュ機構へのアクセスが許可されると、Webサービスへのアクセス制御をしているにもかかわらず、キャッシュ機構を設けたことにより、アクセス権限のクラスに応じて提供される高付加価値情報や、ユーザへの特典がキャッシュ機構を介してアクセス権限のないユーザに対して提供されることになり、高付加価値
20 のWebサービスの有効性やサービスへの誘因提供性が失われてしまうことにもなる。

- このため、キャッシュ機構へのアクセスについてもユーザのアクセス権限に関連して制御する必要が生じることになる。この場合ユーザから
25 のオブジェクト呼出し要求ごとに呼出されるメソッドへのアクセス権限をその度ごとに判断し、キャッシュ機構へのアクセス制御とWebサービス

へのアクセス制御とを同時に実行させるのでは、処理に時間がかかり、キャッシュ機構を設けることによりユーザへの実行結果の表示を高速化するという点では著しい不都合を与えることになる。また、ユーザのアクセス権限が変更されたり、サービス提供者のアクセス条件が変更された場合に、キャッシュ機構へのアクセスにより生じる高付加価値情報のリークに容易に対応することができることが好ましい。このため、ユーザへのWebサービス提供性能の向上という観点からいえば、アクセス制御とキャッシュ機構とを同時に使用して、高い信頼性の下で、可能な限りWebサービスを提供することが望まれていた。

10

本発明は上記従来技術の不都合に鑑みてなされたものであり、本発明は、高い信頼性で、高付加価値のWebサービスを可能な限り迅速に提供することを可能とするWebサービス提供システムを提供することを目的とする。さらに本発明は、コンピュータ・システムを上述したWebサービスを提供することができるサーバ装置装置を提供することを目的とする。さらに本発明は、コンピュータ・システムを上述したサーバ装置装置として機能させることが可能なサーバ装置制御方法を提供することを目的とする。また本発明のさらに別の目的は、コンピュータ・システムを上述したサーバ装置装置として機能させるためのプログラム、および該プログラムを記録したコンピュータ可読な記録媒体を提供することを目的とする。

発明の開示

25 本発明は、Webサービスが許可するオブジェクトをあらかじめ解析しておき、オブジェクトが呼び出すメソッドのアクセス権限を取得してアク

セス権限セットを生成しておく。その後、オブジェクトとアクセス権限
セットとを対応させておくことにより、所定のアクセス権限が付与され
たユーザがWebサービスを要求した場合に、ユーザの要求する要求オブジ
ェクトに対応するアクセス権限セットと、ユーザのアクセス権限とから、
5 キャッシュ機構へのアクセスを許可する機能をサーバ装置装置に付与す
ることができれば、Webサービスの高速性および高信頼性を提供すること
が可能となる、という着想の下になされたものである。

本発明では、上記機能を達成するためにあらかじめJava（登録商標）
10 のコードを解析しておき、所定のサービスの実行を完遂するのに呼び出
される可能性のあるメソッドをすべて列挙する。一方で、列挙されたメ
ソッドすべてのアクセス権限をリストして、オブジェクトに対するアク
セス権限セットのリスト（以下、オブジェクトーアクセス権限リストと
して参照する。）をあらかじめ生成し、格納しておく。このリストを使
15 用して要求オブジェクトに対するWebサービスを要求したユーザのアクセ
ス権限を判断し、リストにより許可されるユーザにのみキャッシュ機構
に対するアクセスを許可し、実行結果（以下、キャッシュ・エントリと
して参照する。）として格納された過去に実行されたオブジェクトの実
行結果を返す。本発明のサーバ装置装置によれば、キャッシュ機構が本
20 来的に許可されないメソッドの実行結果に対応するキャッシュ・エント
リの値を、ユーザに対して返してしまうことはない。また、キャッシュ
された過去の実行結果が得られない場合には、キャッシュ機構は、ユー
ザからのオブジェクト呼出し要求をオブジェクトの実行部に渡し、その
実行結果をアクセス権限の範囲内でユーザに取得させることが可能とな
25 る。

- 本発明では、上記の機能をサーバ装置装置に対して付与するために、Webサービスを実行させるオブジェクトを解析し、呼び出される可能性のあるメソッドに対応したアクセス権限を取得することで、オブジェクトの実行に必要なアクセス権限セットを抽出する手段を提供する。生成されたアクセス権限セットは、オブジェクトごとに対応づけられたリストとして格納され、ユーザがキャッシュ・エントリにアクセス可能かどうかを判定するために読出され、キャッシュ・エントリに対するユーザのアクセス可否が決定される。
- 10 上述したオブジェクト解析では、必要なアクセス権限を抽出する、具体的には、EJBのようなコードと設定ファイルとがパッケージ化されたオブジェクト・プログラムを対象として、所定のオブジェクトを呼出す際に呼出されるすべてのメソッドが特定される。ついで、それらのメソッドに与えられたアクセス権限を集めてアクセス権限セットのリストを構成させる処理を実行する。本発明によれば、アプリケーションに応じて呼出しが行われる可能性のあるすべてのメソッドに対するアクセス権限を保有するユーザに対してのみ、キャッシュ・エントリへのアクセスが許可され、高信頼性を提供することができる。
- 20 さらに本発明では、キャッシュ機構とオブジェクト解析機構とが完全に独立しているので、解析された情報に基づいて、管理者の責任においてキャッシュ機構に条件を緩めて必要なユーザ権限を設定することも可能であるし、さらには、ユーザのアクセス権限のアップグレードや、ダウングレードに伴う変更に対しても、ユーザの変更後のアクセス権限を変更するだけで、キャッシュ機構へのアクセス機構に対してなんらの付加的な機構を設けることなく、高速、かつ高信頼性のWebサービスを提供
- 25

することが可能となる。

すなわち、本発明によれば、ネットワークを介してWebサービスを提供するためのサーバ装置を含むWebサービス提供システムであって、前記サ

5 ーバ装置は、

前記ネットワークを介して受信したオブジェクト呼出し要求と、ユーザ識別子とを取得すると共に、取得したオブジェクト呼出し要求を格納させ、かつ前記ユーザ識別子により指定されるアクセス権限と、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限

10 セットとを比較する制御手段と、

過去に実行されたオブジェクトの実行結果を格納する記憶部とを含み、前記制御手段は、前記記憶部が過去に実行された前記要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワ

15 ークを介して前記サーバ装置の外部に送信する、Webサービス提供システムが提供される。

本発明では、前記制御手段は、前記ユーザ識別子により指定されるアクセス権限が前記アクセス権限セットに含まれる場合に、前記記憶部の
20 検索を実行させることができる。また、本発明では、前記サーバ装置はさらに、オブジェクト実行手段を含み、前記制御手段は、前記記憶部に該当する過去の実行結果が格納されていない場合に、前記オブジェクト呼出し要求をオブジェクト実行部に送り前記要求オブジェクトを実行させることができる。本発明においては、前記サーバ装置は、前記制御手
25 段を含むエッジ・サーバと、前記オブジェクト実行部を含むアプリケーション・サーバとから構成されていてもよい。

本発明によれば、ネットワークを介してWebサービスを提供するためのサーバ装置であって、前記サーバ装置は、

- オブジェクト呼出し要求を受取り、かつ格納させると共に、要求オブジェクトへのアクセス権限と、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限セットとを比較する制御手段と、過去に実行されたオブジェクトの実行結果を格納する記憶部とを含み、

- 前記制御手段は、前記記憶部が過去に実行された前記要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信する、サーバ装置が提供される。本発明では、前記制御手段は、前記ユーザ識別子により指定されるアクセス権限が前記アクセス権限セットに含まれる場合に、前記記憶部の検索を実行させることができる。

さらに、本発明によれば、ネットワークを介してWebサービスを提供するためのサーバ装置であって、前記サーバ装置は、

- 要求オブジェクトが呼出す可能性のあるメソッドすべてを取得してアクセス権限セットを生成するオブジェクト・アナライザ手段と、前記要求オブジェクトを実行するためのオブジェクト実行手段と、過去のオブジェクトの実行結果を格納する記憶部を含んで構成され、かつ前記アクセス権限セットを使用して前記オブジェクト呼出し要求に応答して前記記憶部に対するアクセス制御を実行するキャッシュ機構とを含むサーバ装置が提供される。

本発明における前記キャッシュ機構は、
要求管理部と、

前記記憶部に格納された過去の要求オブジェクトの実行結果の検索を
制御するアクセス制御部とを含んで構成することができる。本発明では、

- 5 前記アクセス制御部は、前記要求オブジェクトに対するアクセス権限と、
前記アクセス権限セットとを比較してアクセス制御を実行し、

前記要求管理部は、前記アクセス制御部の判断に応答して前記オブジ
ェクト呼出し要求を前記オブジェクト実行部へと渡して前記要求オブジ
ェクトの実行を制御することができる。本発明では、前記オブジェクト・

- 10 アナライザ手段は、さらにオブジェクトのコードから前記オブジェクト
が呼出す可能性のあるメソッドを取得する手段と、該メソッドに対応す
るアクセス権限を取得する手段と、前記オブジェクトが呼び出す可能性
のあるすべてのメソッドへのアクセス権限から前記アクセス権限セット
を生成して格納させる手段とを含むことができる。

15

本発明によれば、コンピュータ・システムを、ネットワークを介してW
ebサービスを提供するためのサーバ装置として機能させるためのサーバ
制御方法であって、前記方法は、前記コンピュータ・システムに対して、

- 20 オブジェクト呼出し要求を受信し格納するステップと、
要求オブジェクトへのアクセス権限をメモリから取得するステップと、

前記要求オブジェクトの実行を行うためのアクセス権限セットをメモ
リから読出すステップと、

- 25 前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断
するステップと、

前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記要求オブジェクトの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索させるステップと

を実行させる、サーバ制御方法が提供される。

5

また、本発明では、前記記憶部が過去に実行された要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信するステップを実行させることができる。さらに本発明では、前記記憶部が過去に実行された要求オブジェクトの実行結果を格納しない場合には、前記オブジェクト呼出し要求をオブジェクト実行部へと渡すステップを実行させることができる。

本発明によれば、コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムは、前記コンピュータ・システムに対して、

オブジェクト呼出し要求を受信し格納するステップと、
要求オブジェクトへのアクセス権限をメモリから取得するステップと、

20

前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、

前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、

25 前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記アプリケーションの実行前に過去のオブジェクトの実行結果を格納し

た記憶部を検索させるステップと

を実行させる、プログラムが提供される。

また、本発明によれば、コンピュータ・システムを、ネットワークを
5 介してWebサービスを提供するためのサーバ装置として機能させるための
プログラムを記憶したコンピュータ可読な記憶媒体であって、前記プロ
グラムは、前記コンピュータ・システムに対して、

オブジェクト呼出し要求を受信し格納するステップと、

要求オブジェクトへのアクセス権限をメモリから取得するステップと、

10

前記要求オブジェクトの実行を行うためのアクセス権限セットをメモ
リから読出すステップと、

前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断
するステップと、

15 前記アクセス権限が前記アクセス権限セットに含まれる場合には、前
記アプリケーションの実行前に過去のオブジェクトの実行結果を格納し
た記憶部を検索させるステップと

を実行させる、コンピュータ可読な記憶媒体が提供される。

本発明によれば、コンピュータ・システムをネットワークを介してWe
bサービスを提供するためのサーバ装置として機能させるためのプログラ
ムであって、前記プログラムは、前記コンピュータ・システムに対して、

要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアク
25 セス権限から生成されるアクセス権限セットをメモリから読出すステッ
プと、

前記要求オブジェクトに対する所与のアクセス権限と前記アクセス権限セットとを使用して記憶部に格納されたオブジェクトの過去の実行結果へのアクセスを制御するステップと

を実行させるプログラムが提供される。

5

また、本発明によれば、コンピュータ・システムをネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムを記憶したコンピュータ可読な記憶媒体であって、前記プログラムは、前記コンピュータ・システムに対し

10 て、

要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限から生成されるアクセス権限セットをメモリから読出すステップと、

前記要求オブジェクトに対する所与のアクセス権限と前記アクセス権限セットとを使用して記憶部に格納されたオブジェクトの過去の実行結果へのアクセスを制御するステップと

15

を実行させる記憶媒体が提供できる。

図面の簡単な説明

20

図1は、本発明のWebサービス提供システムの概略的な構成を示した図。

図2は、本発明のサーバ装置装置の機能ブロックを示した図。

25 図3は、本発明のオブジェクト・アナライザの機能ブロックを示した図。

図 4 は、本発明のキャッシュ機構における処理を示したフローチャート。

- 5 図 5 は、本発明のキャッシュ機構におけるキャッシュ・エントリが見出されなかった場合の処理を示したフローチャート。

図 6 は、本発明におけるユーザーアクセス権限テーブルの実施の形態を示した図。

10

図 7 は、本発明におけるオブジェクトアクセス権限リストの実施の形態を示した図。

図 8 は、本発明のメソッドアクセス権限テーブルの実施の形態を示し

15 た図。

図 9 は、本発明におけるキャッシュ・エントリの構成を示した図。

図 10 は、本発明におけるアクセス権限セット生成処理を示した概略図。

20

図 11 は、本発明におけるオブジェクト・アナライザにおける処理を示したフローチャート。

- 25 図 12 は、本発明におけるオブジェクト・アナライザにおける処理を示したフローチャート。

図 1 3 は、図 1 1 および図 1 2 に示したオブジェクト・アナライザにおける本質的な処理部分の擬似コードの実施の形態を示した図。

- 5 図 1 4 は、本発明のオブジェクト・コード解析の他の実施の形態を示した概略図。

図 1 5 は、本発明のアクセス権限判断を実行させる処理のフローチャート。

10

図 1 6 は、図 1 5 に示したアクセス権限判断を実行させるための擬似コードの実施の形態を示した図。

- 図 1 7 は、本発明のWebサービス提供システムのトランザクションの実施
15 の形態を示した図。

図 1 8 は、本発明のWebサービス提供システムのトランザクションの実施の形態を示した図。

- 20 図 1 9 は、本発明のWebサービス提供システムのトランザクションの実施の形態を示した図。

図 2 0 は、本発明のサーバ装置装置の他の実施の形態を示した図。

- 25 図 2 1 は、従来のアクセス制御機構を含むWebサービス提供システムの処理を示した図。

図 2 2 は、従来のアクセス制御機構を含むWebサービス提供システムの処理を示した図。

- 5 図 2 3 は、従来のアクセス制御機構とキャッシュ機構とを含むWebサービス提供システムの処理を示した図。

発明を実施するための最良の態様

以下、本発明を図面に示した具体的な実施の形態に基づいて説明する

- 10 が、本発明は、後述する実施の形態に限定されるものではない。

A : Webサービス提供システムの概略構成

- 図 1 は、本発明のWebサービス提供システムの概略的な構成を示した図である。図 1 に示したWebサービス提供システム 1 0 は、ユーザ端末 1 2
15 と、サーバ装置 1 4 と、ユーザ端末 1 2 と、サーバ装置 1 4 との間を遠隔的に接続するネットワーク 1 6 とを含んで構成されている。本発明において使用することができるユーザ端末 1 2 としては、デスクトップ・コンピュータ、ノート型コンピュータ、携帯型コンピュータといったコンピュータの他、セルラ電話などを挙げることができる。また、本発明
20 において使用することができるサーバ装置 1 4 としては、パーソナル・コンピュータ、ワークステーションといったコンピュータ・システムを使用することができる。ユーザ端末 1 2 と、サーバ装置 1 4 とを接続するためのネットワーク 1 6 としては、TCP/IP など、これまで知ら
25 き、ISDN、ADSL といった通信回線、無線ネットワーク、地上波通信、衛星通信、およびこれらを任意に組み合わせ、サーバ装置 1 4 へ

のアクセスを可能とする限り、いかなるものでも使用することができる。

ユーザは、図 1 に示した Web サービス提供システムにおいて、サーバ装置 14 から高付加価値のサービスの提供を受けるため、サービス提供者などと契約して、ユーザ ID、パスワードといった認証情報を取得している。ユーザは、Web サービス提供システムにアクセスする場合には、インターネットといったネットワーク 16 にアクセスし、URL アドレスなどを指定してユーザ識別子であるユーザ ID、パスワードなどを入力する。サーバ装置 14 は、アクセス認証の後、特定の URL サイトにおける Web サービスを許可する構成とされている。

本発明における高付加価値のサービスとは、種々のサービスを挙げることができるが、例えばユーザのクラス分け（以下、アクセス権限：role として参照する。）に応じて、順次詳細な情報を提供することができる天気予報サービス、ユーザのクラス分けに応じて金利やメリットが変化する金融サービス、株式情報サービス、医療サービス、エンターテインメント提供サービスなどを挙げることができる。

以下、本発明を具体的に説明するために、Web サービス提供システムは、Servlet/EJB/DB を用いた標準的な 3 tier 構成であるものとし、EJB 部分は、ユーザごとに作られるセッション・ビーンと、各セッションから共通して使われるエンティティ・ビーンからなるものとする。株または天気情報は、特定の実施の形態として、セッション・ビーン、getStockRecommendation()、getWeatherForecast() により提供されており、データベースと結びついている株（天気）エンティティ・ビーン getStockInfo()、g

etDetailedInfo() を呼出してその情報を構築するものとする。

本発明では、ユーザ単位に構成されるためアクセス制御のいらないセッション・ビーンではなく、エンティティ・ビーンの各メソッドにはアクセス権限ベースでのアクセス制御が実行されるものとする。セッション・ビーンによりユーザ認証が実行され処理が進行するものとする。

なお、以下の実施の形態で説明する各メソッドと、アクセス権限との関係は、getDetailedInfo()はGoldのみ、getDetailedStock()はSilverとGoldのみがアクセスできるものとする。また、getWeatherForecast()は、アクセス権限に応じて、Bronze/Silverの場合は、おおまかな天気予報を返すが、Goldの場合は正確な天気予報を返すものとする。さらに、getStockRecommendation()は、アクセス権限に応じて、Bronzeのアクセス権限では、場合は単純な株情報を返すが、SilverとGoldのアクセス権限に対してはgetDetailedStock()を呼出して高度なおすすめ株情報を返すメソッドであるものとする。

サーバ装置 14 へのアクセスが認証されたユーザは、その後、要求するWebサービスを実行するためのオブジェクト呼出し要求をサーバ装置 14 へと送る。サーバ装置 14 は、オブジェクト呼出し要求から要求オブジェクトを特定し、サービスの提供を行なっている。Webサービスに必要とされる情報は、データベース 18 に格納されていて、要求オブジェクトにより検索や、処理が実行され、ユーザへと提示される構成とされている。本発明のサーバ装置 14 は、ユーザに付与されたアクセス権限に基づき要求オブジェクトへのアクセス制御を実行していると共に、ユーザが過去にアクセスしたオブジェクトの実行結果を記憶するキャッシュ

機構を含んで構成されている。このキャッシュ機構は、ユーザが過去にアクセスしたと同一のサービスを同一のアクセス権限、または本発明の他の実施の形態ではより高いクラスのアクセス権限で要求した場合には、キャッシュ機構にキャッシュ・エントリとして格納された実行結果への

5 アクセスが許可される。キャッシュ機構へとアクセスして実行結果の値をユーザに返すまでの処理は、アプリケーションを実際に実行するよりも本発明においては高速である。

このため、キャッシュ機構に格納された実行結果を取得することで、

10 最初に同一のWebサービス提供を要求した場合に比較して、より高速のデータ提供が可能とされている。また、ユーザが初めて要求するオブジェクトの場合には、キャッシュ・エントリを参照しても該当するキャッシュ・エントリがないのでサーバ装置 1 4 において、Webサービスを提供するためのオブジェクトが呼び出され、アクセス権限に対応して各メソッドが実行される。サーバ装置 1 4 は、実行結果をユーザに返すことによりユーザに対してWebサービスを提供すると共に、実行結果をキャッシュ機構の新たなエントリとして追加して格納する。

15

図 2 は、本発明のサーバ装置 1 4 の概略的な機能ブロックを示した図

20 である。図 2 に示すように、本発明のサーバ装置 1 4 は、ネットワーク 1 6 を介して送受信を行うための送受信部 2 0 と、キャッシュ機構 2 2 と、Webサービスを提供するためのオブジェクトを解析してオブジェクトが呼出す可能性のあるメソッドのアクセス権限セットを、メソッドごとのアクセス権限に基づいて生成するオブジェクト・アナライザ 2 4 と、W

25 ebサービスのためのオブジェクト呼出して実行するためのオブジェクト実行部 2 6 とを含んで構成されている。キャッシュ機構 2 2 は、受信し

たオブジェクト呼出し要求とユーザに与えられた所与のアクセス権限とアクセス権限セットとに基づいて、キャッシュ機構 22 に格納されたキャッシュ・エントリの検索を可能とさせている。

- 5 オブジェクト・アナライザ 24 は、本発明の特定の実施の形態では、オブジェクト実行部 26 が使用する EJB といったオブジェクトのコードを解析し、コード上で呼出しが行われる可能性のあるメソッドを取得する。この解析は、EJB における構文を解析して、呼びされるメソッドをたとえば、ハッシュ・テーブルに格納するなどにより実行される。その後、取得したメソッドに対応するアクセス権限を、メソッドに割当てられたアクセス権限をリストした、メソッドーアクセス権限テーブルをルックアップして取得し、オブジェクトを実行させるためのアクセス権限をすべて取得する。すべてのアクセス権限を取得した後、オブジェクト・アナライザ 24 は、オブジェクトーアクセス権限リストを生成し、生成されたアプリケーションーアクセス権限リストは、例えば適切なメモリ 38 に登録される。
- 10
- 15

- オブジェクト実行部 26 は、ハードディスクといった記憶手段 28 に格納されたオブジェクトを適切なメモリに呼出して実行させ、ユーザから要求されたオブジェクトに対する実行結果を生成し、生成した実行結果をメモリ 38 に渡している。キャッシュ機構 22 は、メモリ 38 から実行結果を読み出して、要求オブジェクトの実行結果をユーザに提供すると共に、新たなキャッシュ・エントリとして格納させ、将来のユーザ要求に対して高速な Web サービスの提供を可能とさせている。
- 20

図 2 に示したキャッシュ機構 22 は、さらに詳細には要求管理部 30

と、アクセス制御部 3 2 と、記憶部 3 4 とを含んで構成されている。図 2 に示されたキャッシュ機構 2 2 は、要求管理部 3 0 と、アクセス制御部 3 2 とがサーバ装置 1 4 内に配置されていて、記憶部 3 4 への制御手段を構成している。また、図 2 では、記憶部 3 4 は、図面上ではサーバ装置 1 4 の外部に配置されているものの、サーバ装置 1 4 における内蔵ハードディスクなどを使用することができる。要求管理部 3 0 は、ユーザから送られたユーザ ID をキーとして、ユーザーアクセス権限テーブルをルックアップし、ユーザに与えられた所与のアクセス権限を取得する。また、ユーザが送信するオブジェクト呼出し要求のデータから、ユーザが希望するサービスを実行するオブジェクトを特定し、特定されたオブジェクトを一義的に指定するため、例えばオブジェクト呼出し要求をテキスト・コードとし、当該テキスト・コードを識別子として使用することができる。以下、本発明においてはオブジェクト識別子として、オブジェクト名を使用するものとして説明を行うが、本発明においては他のいかなる識別手法を使用することもできる。オブジェクト名は、その後アクセス制御部 3 2 へと渡される。アクセス制御部 3 2 は、ユーザが保有するアクセス権限を、メモリ 3 8 に格納されたオブジェクト→アクセス権限リストを讀出して比較を行い、ユーザが保有するアクセス権限が、ユーザが要求された要求オブジェクトに該当するか否かを判断する。

ユーザが要求した要求オブジェクトがユーザのアクセス権限で利用が認められる場合には、アクセス制御部 3 2 は、ユーザが要求したオブジェクト名に対応するキャッシュ・エントリ 3 6 を検索させる。該当するキャッシュ・エントリ 3 6 a が見出された場合には、キャッシュ・エントリ 3 6 a の値をアクセス制御部 3 2 へと渡して、ユーザへと実行結果

として提供し、さらに後続するユーザからの要求に対応する。また、ユーザが錯誤または意図的にアクセス権限のないオブジェクトの要求を行った場合には、アクセス制御部 32 は、ユーザのアクセス権限を、オブジェクトアクセス権限リストと比較して、正当なアクセス権限がない
5 ものと判断し、要求管理部 30 に対してアクセスを許可しない通知を行う。この通知は、アクセス不可フラグを送信するなど、これまで知られたいかなる方法でも使用することができる。

また、本発明の他の実施の形態では、ブラウザ・ソフトウェアを介し
10 て、ユーザに、アクセス権限がないのでWebサービスにアクセスできないことを表示することもできる。また、ユーザが適切なアクセス権限を保有しているが記憶部 34 に該当するキャッシュ・エントリが見出されない場合には、要求管理部 30 へとキャッシュ・エントリなしの通知が送られる。要求管理部 30 は、その通知を受け取ると、適切なメモリ、例
15 えばメモリ 38 に一時的に格納しておいたユーザが要求したオブジェクト呼出し要求を、オブジェクト実行部 26 へと渡す。オブジェクト実行部 26 は、オブジェクトを呼出して実行させ、ユーザが要求した実行結果を生成する。生成された実行結果は、メモリ 38 へと格納される。要求管理部 30 は、格納された実行結果を読み出し、Netscape Navigator (
20 商標) や、Internet Explorer (商標) といったブラウザ・ソフトウェアを使用して、ユーザに対して提供することができる構成とされている。

図 3 は、本発明のオブジェクト・アナライザ 24 の概略構成を示した図である。本発明におけるオブジェクト・アナライザ 24 は、入力バッ
25 ファ 40 と、パーサ 42 と、メソッドアクセス権限テーブル 44 と、アクセス権限セット生成部 46 とを含んで構成されている。オブジェク

ト・アナライザ 24 は、入力バッファ 40 にオブジェクト実行部 26 が使用するオブジェクトを記憶手段 28 からあらかじめ取得させ、入力バッファ 40 に格納されたオブジェクトを、パーサ 42 へと渡して、オブジェクトのコードを解析させる。解析の結果、オブジェクトに呼出される可能性のあるメソッドが取得されると、メソッドを適切なメモリに格納する。

オブジェクト・アナライザ 24 は、メモリからメソッドを讀出して、メソッド・アクセス権限テーブル 44 をルックアップし、当該メソッド
10 に対して、Webサービス提供者により指定されたアクセス権限を取得し、アクセス権限セット生成部 46 に渡す。アクセス権限セット生成部 46 は、渡されたメソッドごとのアクセス権限を使用して、所定のオブジェクトに対応するアクセス権限セットを生成する。生成されたアクセス権限セットは、出力バッファ 48 へと一時的に格納される。オブジェクト・
15 アナライザ 24 は、出力バッファ 48 に蓄積されたアクセス権限セットを、メモリ 38 へとオブジェクト名と対応させて格納させることにより、オブジェクト・アクセス権限リストを生成させる。

本発明においては、上述したオブジェクト・アナライザ 24 を設け、
20 オブジェクトの呼出しにより呼出される可能性のあるメソッドとアクセス権限とをあらかじめ取得しておき、オブジェクト・アクセス権限リストとして適切なメモリ、例えばメモリ 38 に登録する。このため、Webサービスを提供するオブジェクトが新たに追加されるまでオブジェクト・アクセス権限リストの再構築をする必要がなく、高速のアクセス判断を
25 可能とする。また、さ新たにWebサービスに対応するオブジェクトが追加された場合でも、実際にオブジェクトがユーザにより要求される前に解

析しておくことが可能なので、オブジェクト・プログラムの追加があった場合にでも、最小のコストで、高速かつ高信頼性のWebサービスを提供することが可能となる。

5 B：本発明のキャッシュ機構の実行する処理

図4は、本発明におけるキャッシュ機構の処理のフローチャートを示した図である。本発明におけるキャッシュ機構の処理は、ステップS10においてユーザからのオブジェクト呼出し要求を受信して、要求オブジェクト名を特定する。次いで、取得された要求オブジェクト名は、ステップS12において適切なメモリに格納される。ステップS14では、先だって送られた、またはオブジェクト呼出し要求と共に送られたユーザIDをキーとして、ユーザーアクセス権限テーブルをルックアップさせることでユーザに与えられたアクセス権限を取得し、メモリに登録する。ステップS16では、取得されたユーザのアクセス権限と、オブジェクト名とを使用して、オブジェクトアクセス権限リストのエントリをメモリから読み出し、比較する。

ステップS16における比較の結果、要求されたオブジェクトがユーザのアクセス権限で実行可能な場合 (yes) には、ステップS18に進む。ステップS18では、オブジェクト名を検索キーとして使用して記憶部34に格納されたキャッシュ・エントリの検索を実行させる。ステップS18で、キャッシュ・エントリが見出された場合 (yes) には、ステップS20において、キャッシュ・エントリが見出されたことをアクセス制御部に通知する。ステップS22では、検索された実行結果を受け取ったアクセス制御部は、要求処理部へと通知して、キャッシュ・エントリの値を取得させ、ブラウザ・ソフトウェアを使用してユーザに提示して、

Webサービスの提供を可能とする。

また、ステップS 1 6においてユーザのアクセス権限がオブジェクト
ーアクセス権限リストにより記憶部3 4へのアクセス可ではないと判断
5 された場合(no)には、ステップS 2 4でアクセス制御部にアクセスが拒
否されたことが通知される。また、本発明の説明している実施の形態で
は、ステップS 2 6において要求処理部からユーザへとアクセスが拒否
されたことが通知されている。同時に、要求差オブジェクト呼出し要求
は、キャッシュ機構内から廃棄される。

10

図5は、図4のステップS 1 8でキャッシュ・エントリが見出されな
かった場合(no)の詳細な処理を示した図である。ステップS 1 8でキャ
ッシュ・エントリが見出されなかった場合(no)には、ステップS 2 8で
アクセス制御部に通知を行い、ステップS 3 0において適切なバッファ・
15 メモリに格納しておいたオブジェクト呼出し要求をオブジェクト実行部
へと渡す。オブジェクト呼出し要求を受け取ったオブジェクト実行部は、
要求オブジェクトを呼出して実行させ、実行結果を適切なメモリ、例え
ばメモリ3 8に格納する。ステップS 3 2において要求処理部は、実行
結果をメモリ3 8から読出し、ステップS 3 4で実行結果をブラウザ・
20 ソフトウェアを使用してユーザに提供する。また、ステップS 3 6では、
実行結果がオブジェクト名とアクセス権限セットとが適切なメモリ領域
から読出され、ステップS 3 8でオブジェクト名と、アクセス権限セッ
トと、実行結果とが記憶部における新たなキャッシュ・エントリとして
登録される。

25

C : キャッシュ機構が使用するデータ構成

図6は、本発明のアクセス制御部32が使用するユーザーアクセス権限テーブルのデータ構成を示した図である。ユーザーアクセス権限テーブルは、図6に示すように、ユーザを特定するためのユーザIDと、それに対応するアクセス権限(Gold、Silver、Bronze)とが対として構成されている。このテーブルは、Webサービスを提供する者またはサーバ装置管理者により入力され、例えば、ハードディスク28、ユーザ・データベースなどに格納しておくことができる。図6に示したユーザーアクセス権限テーブルは、例えばサーバ装置14が管理する図示しないユーザ・データベースに格納しておくことができる。サーバ装置14がユーザからのユーザIDを受信すると、ユーザIDが適切なメモリに格納され、格納されたユーザIDは、アクセス制御部32により読出され、読み出されたユーザIDをキーとしてユーザーアクセス権限テーブルをルックアップすることにより、ユーザのアクセス権限がアクセス制御部32により取得される。

15

図7は、アクセス制御部32が使用するオブジェクトアクセス権限リストの実施の形態を示した図である。図7では、アクセス権限が、Gold、Silver、Bronzeで示されており、それぞれのオブジェクト1およびオブジェクト2に対するアクセス権限がyesまたはnoで示されている。オブジェクトとしては具体的には上述した天気予報では、getWeatherForecast()とすることができ、株式情報では、getStockRecommendation()とすることができる。オブジェクト1に対してBronzeのアクセス権限に対してyesのアクセス権限を生成するためには、呼出される可能性のあるメソッド1、メソッド2、メソッドzがすべてBronzeのアクセス権限のユーザに対してアクセスできることが必要となる。

25

アクセス制御部 32 は、ユーザから送られたユーザ ID に基づき、図 6 に示したユーザのアクセス権限、Gold、Silver、Bronze を取得した後、オブジェクト識別子をキーとして使用して、図 7 に示したオブジェクト
5 アクセス権限リストをルックアップする。その後、オブジェクトと要求されたメソッドとをルックアップして比較を行い、呼び出されるメソッドのうちの 1 つでもアクセス権限が no となる場合には、アクセス許可フラグを設定しないなどにより、記憶部 34 へのキャッシュ・アクセスを実行させない。なお、「キャッシュ・アクセス可」は、記憶部 34 を参照できると共に、新たなデータを記憶部 34 に書込むことができるこ
10 とを意味する。また、アクセス権限セットは、図 7 に示した 1 つのアプリケーションに対する縦方向のコラムが、アクセス権限セットの具体的な要素を示している。

図 8 は、本発明のオブジェクト・アナライザ 24 が使用することがで
15 きる、メソッド・アクセス権限テーブルの実施の形態を示す。メソッド・アクセス権限テーブルは、オブジェクトが呼び出す可能性のあるメソッドと、当該メソッドを実行することができるアクセス権限、例えば Gold、Silver、Bronze とが対として登録されたテーブルとして構成することができる。このテーブルは、サービス提供者やサーバ装置管理者など
20 により作成され、例えば、データベース 28 や、ユーザ・データベースなどに格納することができる。

図 9 は、記憶部 34 が格納するキャッシュ・エントリの具体的な構成を示した図である。図 9 に示されるように、記憶部 34 は、過去にアクセスされた Web サービスを実行させるためのオブジェクト名と、アクセス
25 権限セットと、対応するオブジェクトの実行結果とがキャッシュ・エン

トリ 3 6 を構成している。オブジェクト呼出し要求を受信して、キャッシュ・アクセス可と判定されたユーザ要求は、アクセス制御部 3 2 により、オブジェクトを実行するに先立って対応するオブジェクト名をキーとして記憶部 3 4 をルックアップして、該当するキャッシュ・エントリ 5 の検索が実行される。該当するキャッシュ・エントリ 3 6 a が検索された場合には、検索された実行結果がブラウザ・ソフトウェアを使用してユーザへと提供される。検索されなかった場合には、その通知がアクセス制御部 3 2 へと送られ、その後に得られた要求オブジェクトの実行結果の値が、実行されたオブジェクトのオブジェクト名、アクセス権限セ
10 ットと共にキャッシュ・エントリ 3 6 b として格納される。

D : オブジェクト・アナライザにおける詳細処理

本発明のオブジェクト・アナライザ 2 4 は、Webサービスを実行するためのオブジェクトが呼び出す可能性のあるメソッドごとにアクセス権限
15 を判断し、オブジェクト・アクセス権限リストを生成する。図 1 0 には、本発明のオブジェクト・アナライザ 2 4 の概略的な処理を示す。図 1 0 (a) には、呼び出されるメソッド m_1 と、メソッド m_1 がさらに呼び出す可能性のあるメソッド $n_1() \sim n_i()$ についてのアクセス権限を示している。これらのメソッドに対するアクセス権限は、図 8 で示したメソッド・アクセス権限テーブルにより与えられる。所定のメソッド m_1 に対するアクセス権限は、Webサービス提供者により与えられるメソッド m_1 についてのアクセス権限である $permission(m)$ 、例えば Gold、Silver、Bronze、A、X、Y、Z と、メソッドが呼び出す可能性のあるメソッド $n_1() \sim n_i()$ に付与されたアクセス権限、例えばメソッド $n_1()$ についていえば、 $\{B, S\}$, $\{S,$
20 $G\}$ とされている。

- なお、 $\{\{B, S\}, \{S, G\}\}$ は、メソッド $m_1()$ にアクセスするためには、アクセス権限が、BまたはSおよびアクセス権限がSまたはGであることを必要とすることを意味する。図10(a)では、メソッド m_1 には、 $\{G, A\}$ のアクセス権限が設定され、メソッド m_1 が呼び出しを行う可能性bのあるメソッド $n_1 \sim n_i$ へのアクセス権限がすべて満たされなければメソッド m_1 へのアクセスは認めない。この処理を行った後、結果として生成されるメソッド m_1 へのアクセスが認められるためのアクセス権限セットを $requires(m_1)$ で表すと、 $requires(m_1) = \{\{B, S\}, \{G\}, \{X\}, \{Y, Z\}\}$ が得られる。
- 上述した $requires$ が、アプリケーション—アクセス権限リストにおける
- 10 アクセス権限セットを与える。図10(b)には、本発明の特定の実施の形態におけるアクセス権限セット $requires(m)$ を得るための論理式を示す。なお、本発明においては、呼び出されるメソッドのうち、アクセス権限が不明である場合には、キャッシュ機構へのアクセスを拒否する構成とすることができる。また、これとは反対に、呼び出されるメソッド
- 15 のアクセス権限が不明である場合には、キャッシュ機構へのアクセスは認めないが、Webサービスの提供だけはできるように構成することもできる。また、図10(b)において、unknownとは、アクセス権限が不明のメソッドを意味し、本発明では、アクセス権限が不明のメソッドがあると、キャッシュ・アクセスを拒否する構成とすることができるし、また
- 20 アクセス権限が不明のメソッドがあっても少なくともWebサービスを実行可能に設定することもできる。このような設定のフレキシビリティは、本願において、オブジェクト・アナライザ24とキャッシュ機構22とを、機能的に完全に分離したことにより可能となる。
- 25 図11は、本発明においてオブジェクト・アナライザ26が実行するアクセス権限をメソッドごとに実行するための処理を示したフローチャ

ートである。オブジェクト・アナライザの処理は、ステップS 5 0から開始し、まず、プログラムが呼び出す可能性のあるメソッドをリストしたメソッド・リスト (todo-list) と、処理を終えたメソッドを格納するための処理済リスト (done-list) とをクリアする。ステップS 5 2では、

5 オブジェクトを解析して得られたメソッドをメソッド・リストに格納する。ステップS 5 4では、メソッド・リストに格納されたメソッドに対して、メソッド・アクセス権限テーブルを参照してアクセス権限を取得する。ステップS 5 6では、メソッド・リストが空になったか否かを判断し、空になった場合 (yes) には、呼び出される可能性のあるメソッド

10 に対する処理は終了したので、ステップS 5 8に進んで生成された最終的なアクセス権限セットを生成させる。また、メソッド・リストが空ではない場合 (no) には、さらに処理を行うメソッドが残されているので、ステップS 5 4に戻り、処理を反復する。

15 図1 2は、図1 1に示したステップS 5 4の処理の詳細なフローチャートを示した図である。処理は、ステップS 6 0から開始し、メソッド・リストからメソッドを抽出する。ステップS 6 2では、抽出されたメソッドにつき、メソッド・アクセス権限テーブルをルックアップしながらメソッドのアクセス権限を取得してメモリに格納する。ステップS 6 4

20 では、抽出したメソッドを処理済リストへと移すと同時に、メソッド・リストから削除する。ステップS 6 6では、メソッド呼出しが行われる可能性のある他のメソッドをメソッド・リストに追加して、ステップS 5 4の判断が、肯定的な結果を返すまで順次処理が実行される。図1 3

25 には、図1 2において説明した処理を実行させるための特定の実施の形態における擬似コードを示すものの、本発明においては、図1 2に示した処理を実行させる擬似コードとしては、同様の機能を達成することが

できるいかなるものでも使用することができる。上述した処理により、本発明においてはコード解析がなされ最終的には、集合変数を含む処理済リストの中にサービスを実行するためにアクセスが必要な（可能性のある）メソッドをすべて列挙することができる。

5

また、本発明の他の態様においては、メソッドのコード中で `invokevirtual` などのメソッド呼出しをとみなう部分を探す方法を採用することにより、フロー解析を直接実行させずにメソッドをメソッド・リストに含ませることができる。本発明の上述した他の態様の処理を図 14 に示す。具体的には、メソッド呼び出しに指定されたオブジェクトの静的なクラスやインターフェースに加え、そのサブクラスについて、呼び出されているメソッドが呼ばれるとみなすことにより、処理を実行させることができる。例えば、天気予報の情報提供サービスで説明した `Weather` 型のオブジェクトに対し `getInfo()` が呼び出され、`Weather` のサブクラスに `WeatherImpl` があるものとする。このとき、`Weather` クラスの `getInfo()` に加えて、`WeatherImpl` クラスの `getInfo()` も呼び出される可能性のあるメソッドであるとみなして、メソッド・リストに含ませることができる。

また、本発明は、コントロール・フロー解析やデータ・フロー解析を行なうことで、これらのフロー解析を実行させないで得られるメソッド群から、呼出される可能性のないメソッド群を取り除く処理を追加することもできる。

E：アクセス制御部におけるアクセス権限判断の詳細処理

図 15 には、本発明のアクセス制御部における詳細な処理のフローチャートを示す。アクセス権限判断の処理は、まずステップ S70 において、アクセス許可フラグを初期化（偽）に設定する。ステップ S72 に

において、要求するオブジェクトにつき、オブジェクト→アクセス権限リストにおけるアクセス権限セットのうちの最初のセットをメモリから読み出す。ステップS 7 4において、ユーザのアクセス権限と、読出されたセットとの比較を実行し、比較結果をメモリに格納させる。ステップ

5 S 7 6において、比較結果をメモリから読出し、値が偽であるか否かを判断する。比較結果が偽である場合 (yes) には、少なくとも1つのセットのアクセス権限をユーザは保有しないので、ステップS 7 8において処理を終了させる。この場合、アクセス許可フラグは、nullのまま保持される。また、比較結果が偽でない場合(no)には、ステップS 8 0にお

10 いてすべてのセットを判断したか否かを判断し、すべてのセットを判断していない場合(no)には、ステップS 7 4に戻って次のセットをメモリから読み出し、ステップS 7 6の判断を実行させる。

ステップS 8 0においてアクセス権限セットすべてを判断した場合 (y

15 es) には、アクセス権限セットを構成するすべてのセットに対してユーザがアクセス権限を保有しているので、ステップS 8 2へと進んで、アクセス許可フラグを設定し、ユーザIDおよびオブジェクトを指定して記憶部3 4へのアクセスを可能とさせる。図1 6は、図1 5に示したフローチャートのうち、ステップS 7 4～ステップS 8 0における判断処

20 理を、ユーザが保有するアクセス権限をpとし、アクセス権限セットが、(A, B)、(B, C)、(X, Y, Z)である場合について実行させる際の擬似コードを示すが、本発明においては図1 3において説明したように、同様の機能を実現するいかなるコーディングでも使用することができる。

図1 7は、本発明のWebサービス提供システムにおけるユーザ端末1 2

と、サーバ装置装置 1 4 との間の要求と応答のシーケンスを示した図である。図 1 7 では、ユーザ端末 1 2 からオブジェクト呼出し要求を発行されており、要求管理部 3 0 は、オブジェクト呼出し要求を受け取って、アクセス制御部 3 2 に対してアクセス権限の判断を要求している。アクセス制御部 3 2 は、ユーザーアクセス権限リストをルックアップして、ユーザのアクセス権限を判断し、アクセス権限があると判断すると、記憶部 3 4 に対してキャッシュ・エントリの検索を実行させる検索要求を発行している。図 1 7 において示した実施の形態では、該当するキャッシュ・エントリが見出されず、nullの応答がアクセス制御部 3 2 に返されている。

アクセス制御部 3 2 は、キャッシュ・エントリがない通知を受け取り、要求管理部 3 0 に対して、オブジェクト呼出し許可の通知を渡す。この通知を受け取った要求管理部 3 0 は、オブジェクト呼出し要求を、オブジェクト実行部 2 6 に渡し、処理を実行させる。実行結果は、要求管理部 3 0 が取得し、要求管理部 3 0 は、実行結果をユーザに提供する。また、アクセス制御部 3 2 は、記憶部 3 4 への格納要求を発行して、新たな実行結果を格納させている。

図 1 8 は、本発明のWebサービス提供システムにおける要求-応答シーケンスの他の実施の形態を示した図である。図 1 8 では、ユーザ端末 1 2 からオブジェクト呼出し要求を発行しており、要求管理部 3 0 は、オブジェクト呼出し要求を受け取って、アクセス制御部 3 2 に対してアクセス権限の判断を要求している。アクセス制御部 3 2 は、ユーザーアクセス権限リストをルックアップしてアクセス権限を判断し、アクセス権限があると判断して記憶部 3 4 に対してキャッシュ・エントリの検索を

実行させる要求を発行している。

図 18 において示した実施の形態では、キャッシュ・エントリが見出され、キャッシュ・エントリの値を要求管理部 30 へと取得させ、キャッシュ・エントリの値がサービス応答の結果としてユーザに提供されている。図 18 に示されるように本発明においては、キャッシュ・エントリの値をユーザに返すまでの間にアクセス権限の判断を実行するので、キャッシュ・エントリへのセキュリティを向上させると共に、ユーザに対する Web サービスの提供を高速化することが可能となる。

10

図 19 は、本発明の Web サービス提供システムにおけるユーザ端末 12 と、サーバ装置 14 との間の要求と応答のシーケンスのさらに他の実施の形態を示した図である。図 19 に示した実施の形態は、例えば、ユーザが以前に Web サービスに対して互いアクセス権限のサービスを受けたものの、その後アクセス権限が変化した場合や、Web サービスの提供者側の理由により、所定のアクセス権限での Web サービスの種類を変更した場合に生じる。

図 19 では、ユーザ端末 12 からオブジェクト呼出し要求を発行している。要求管理部 30 は、オブジェクト呼出し要求を受け取って、アクセス制御部 32 に対してアクセス権限の判断を要求している。アクセス制御部 32 は、ユーザーアクセス権限リストをルックアップしてアクセス権限を判断している。図 19 において示した実施の形態では、該当するキャッシュ・エントリが見出され、キャッシュ・エントリの値がアクセス制御部 32 に返されている。図 19 に示した実施の形態では、アクセス制御部 32 がその時点でのユーザがキャッシュ・エントリにアクセ

20
25

スする権限がないと判断し、キャッシュ・エントリに対するアクセス権限がないアクセス拒否の通知を発行し、要求管理部 30 は、この通知を受け取っている。

- 5 この通知を受け取った要求管理部 30 は、ユーザに対してアクセス拒否を通知している。この通知を受け取ったユーザは、再度別のオブジェクト呼出し要求を送り、サーバ装置 14 は、図 17～図 19 に示した処理を選択的に反復させ、ユーザとのトランザクションを進行させることになる。図 19 に示される実施の形態のように、本発明においては、ユーザ側のアクセス権限の変動および Web サービスの条件変更に対して最小のソフトウェアおよびハードウェア資源で迅速に対応でき、高速、かつ高信頼性の Web サービスの提供を行うことが可能となる。
- 10

本発明の形態では、上述したようにアクセス権限セットとして、単純にアクセス権限を要素に持つ集合を要素とする集合として構成することも可能であるし、アクセス権限を要素に持つ集合 R と S とがあり得る場合に、R のアクセス権限のどれかを持っているならば R のアクセス権限のどれかを保持することが知られている場合、アクセス権限セット R のみを保持するようにすることもできる。例えば、R が {Gold} で、S が {Gold, Silver} の場合には、R のアクセス権限がある場合には S を含ませないようにしてアクセス権限セットを構成させることもできる。

15

20

さらに本発明の他の実施の形態では、サーバ装置装置の管理者が、サービスが Web サービスのオブジェクトのコード解析結果に関わらず、そのサービスの結果をキャッシュさせるように指定することができる。

25

- 例えば、あるメソッドgetWeatherForecast()は、コード解析を用いるとアクセス制御機構によりキャッシュ結果を返してはいけないという判定が下されたとする。この場合には通常では、getWeatherForecast()のリクエストに対しては常に実際にWebサービス・オブジェクトが呼び出される。このような場合でも、管理者が特定の限定されたユーザに対して「getWeatherForecast()の結果はキャッシュしてよい」という指定をアプリケーション・サーバ装置に与えることによって、後続するgetWeatherForecast()のリクエストに対してキャッシュされた結果が返されるようにすることを可能とする。キャッシュ機構はこのような設定が与えられている場合には、本発明では、オブジェクト・アナライザと、アクセス制御部とが独立して構成されているので、要求に対応するキャッシュ・エントリがあったときはアクセス制御部の判断によらず、キャッシュ・エントリの値を実行結果としてユーザに返す構成とすることもできる。
- 図20には、本発明のさらに別の実施の形態を示す。図20に示した本発明の他の実施の形態では、エッジ・サーバ装置50に記憶部34として使用することもできる。すなわち、本発明の可能な実施の形態では、本発明のキャッシュ機構は、アプリケーション・サーバ装置52とは別のエッジ・サーバ装置50に配置される。このようなエッジ・サーバ装置50は、ユーザとアプリケーション・サーバ装置52との間に配置されることで、ユーザに対し複数のアプリケーション・サーバ装置への統一したインターフェースを提供することができる。エッジ・サーバ装置50は、ユーザからの要求を受け付け、その要求に含まれる処理をアプリケーション・サーバ装置52に依頼し、エッジ・サーバ装置50に戻された結果をユーザへと返す構成とすることができる。

エッジ・サーバ装置のキャッシュ機構 22 は、上述したアプリケーション・サーバ装置 52 の結果をキャッシュしておき、ユーザ要求に応じてキャッシュされた結果を返す構成とすることもできる。上述したエッジ・サーバ装置におけるアクセス制御つきキャッシュ機構においても、

5 サーバ装置装置 12 内に含ませたキャッシュ機構と処理の実施の形態は、大きく変わるものではなく、キャッシュ機能 22 と、プログラム実行部 24 との間の通信が、例えば TCP/IP プロトコルを介したインターネットや、LAN、WAN といったネットワークを介して行われている。

10

本発明の上述した各機能を実現する手段または部分は、コンピュータ実行可能なプログラム言語により記述されたソフトウェアまたはソフトウェア・モジュール群として構成することができ、必ずしも図面に記載した機能ブロックとして構成される必要はない。また、本発明の Web サービス提供システムでは、要求されるテーブルは必要に応じていかなる機能モジュールと共に構成することができ、本発明の図面に示された特定の実施の形態に限定されるものではない。

15

本発明のプログラムは、種々のプログラミング言語、例えば Java（登録商標）Beans などを使用して記述することができ、本発明のプログラムを記述したコードは、磁気テープ、フレキシブル・ディスク、ハードディスク、コンパクト・ディスク（CD）、光磁気ディスク、デジタル・バーサタイル・ディスク（DVD）といったコンピュータ可読な記録媒体に保持させることができる。

20

25

上述したように、本発明は、高い信頼性で、高付加価値の Web サービス

- を可能な限り迅速に提供することを可能とするWebサービス提供システムを提供することを可能とする。さらに本発明は、コンピュータ・システムを上述したWebサービスを提供することができるサーバ装置装置を提供することを可能とする。さらに本発明は、コンピュータ・システムを上述したサーバ装置装置として機能させることが可能なサーバ装置制御方法を提供することを可能とする。また本発明のさらに別の目的は、コンピュータ・システムを上述したサーバ装置装置として機能させるためのプログラム、および該プログラムを記録したコンピュータ可読な記録媒体を提供することを可能とする。
- 5

請求の範囲

1. ネットワークを介してWebサービスを提供するためのサーバ装置を含むWebサービス提供システムであって、前記サーバ装置は、前記ネットワークを介して受信したオブジェクト呼出し要求と、ユーザ識別子とを取得すると共に、取得したオブジェクト呼出し要求を格納させ、かつ前記ユーザ識別子により指定されるアクセス権限と、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限セットとを比較する制御手段と、過去に実行されたオブジェクトの実行結果を格納する記憶部とを含み、前記制御手段は、前記記憶部が過去に実行された前記要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信する、Webサービス提供システム。
2. 前記制御手段は、前記ユーザ識別子により指定されるアクセス権限が前記アクセス権限セットに含まれる場合に、前記記憶部の検索を実行させる、請求項1に記載のWebサービス提供システム。
3. 前記サーバ装置はさらに、オブジェクト実行手段を含み、前記制御手段は、前記記憶部に該当する過去の実行結果が格納されていない場合に、前記オブジェクト呼出し要求をオブジェクト実行部に送り前記要求オブジェクトを実行させる、請求項1に記載のWebサービス提供システム。
4. 前記サーバ装置は、前記制御手段を含むエッジ・サーバと、前記

オブジェクト実行部を含むアプリケーション・サーバとから構成される、請求項 3 に記載の Web サービス提供システム。

5. ネットワークを介して Web サービスを提供するためのサーバ装置であって、前記サーバ装置は、オブジェクト呼出し要求を受取り、かつ格納させると共に、要求オブジェクトへのアクセス権限と、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限セットとを比較する制御手段と、過去に実行されたオブジェクトの実行結果を格納する記憶部とを含み、前記制御手段は、前記記憶部が過去に実行された前記要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信する、サーバ装置。
6. 前記制御手段は、前記ユーザ識別子により指定されるアクセス権限が前記アクセス権限セットに含まれる場合に、前記記憶部の検索を実行させる、
- 請求項 5 に記載のサーバ装置。
7. ネットワークを介して Web サービスを提供するためのサーバ装置であって、前記サーバ装置は、要求オブジェクトが呼出す可能性のあるメソッドすべてを取得してアクセス権限セットを生成するオブジェクト・アナライザ手段と、前記要求オブジェクトを実行するためのオブジェクト実行手段と、過去のオブジェクトの実行結果を格納する記憶部を含んで構成され、かつ前記アクセス権限セットを使用して前記オブジェクト呼出し要求に応答して前記記憶部に対するアクセス制御を実行するキャ

ッシュ機構とを含むサーバ装置。

8. 前記キャッシュ機構は、要求管理部と、前記記憶部に格納された過去の要求オブジェクトの実行結果の検索を制御するアクセス制御部と
- 5 を含んで構成される請求項7に記載のサーバ装置。

9. 前記アクセス制御部は、前記要求オブジェクトに対するアクセス権限と、前記アクセス権限セットとを比較してアクセス制御を実行し、前記要求管理部は、前記アクセス制御部の判断に応答して前記オブジェ
- 10 クト呼出し要求を前記オブジェクト実行部へと渡して前記要求オブジェクトの実行を制御する、請求項8に記載のサーバ装置。

10. 前記オブジェクト・アナライザ手段は、さらにオブジェクトのコードから前記オブジェクトが呼出す可能性のあるメソッドを取得する
- 15 手段と、該メソッドに対応するアクセス権限を取得する手段と、前記オブジェクトが呼び出す可能性のあるすべてのメソッドへのアクセス権限から前記アクセス権限セットを生成して格納させる手段とを含む請求項7に記載のサーバ装置。

- 20 11. 前記キャッシュ機構を含むエッジ・サーバと、前記オブジェクト実行手段と、前記オブジェクト・アナライザ手段とから構成されるアプリケーション・サーバとを含んで構成される、請求項7に記載のサーバ装置。

- 25 12. コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのサーバ制御方法で

あって、前記方法は、前記コンピュータ・システムに対して、オブジェクト呼出し要求を受信し格納するステップと、要求オブジェクトへのアクセス権限をメモリから取得するステップと、前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、

- 5 前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記要求オブジェクトの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索させるステップとを実行させる、サーバ制御方法。

10

13. 前記記憶部が過去に実行された要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信するステップを実行させる、請求項12に記載の方

15 法。

14. 前記記憶部が過去に実行された要求オブジェクトの実行結果を格納しない場合には、前記オブジェクト呼出し要求をオブジェクト実行部へと渡すステップを実行させる、請求項12に記載の方法。

20

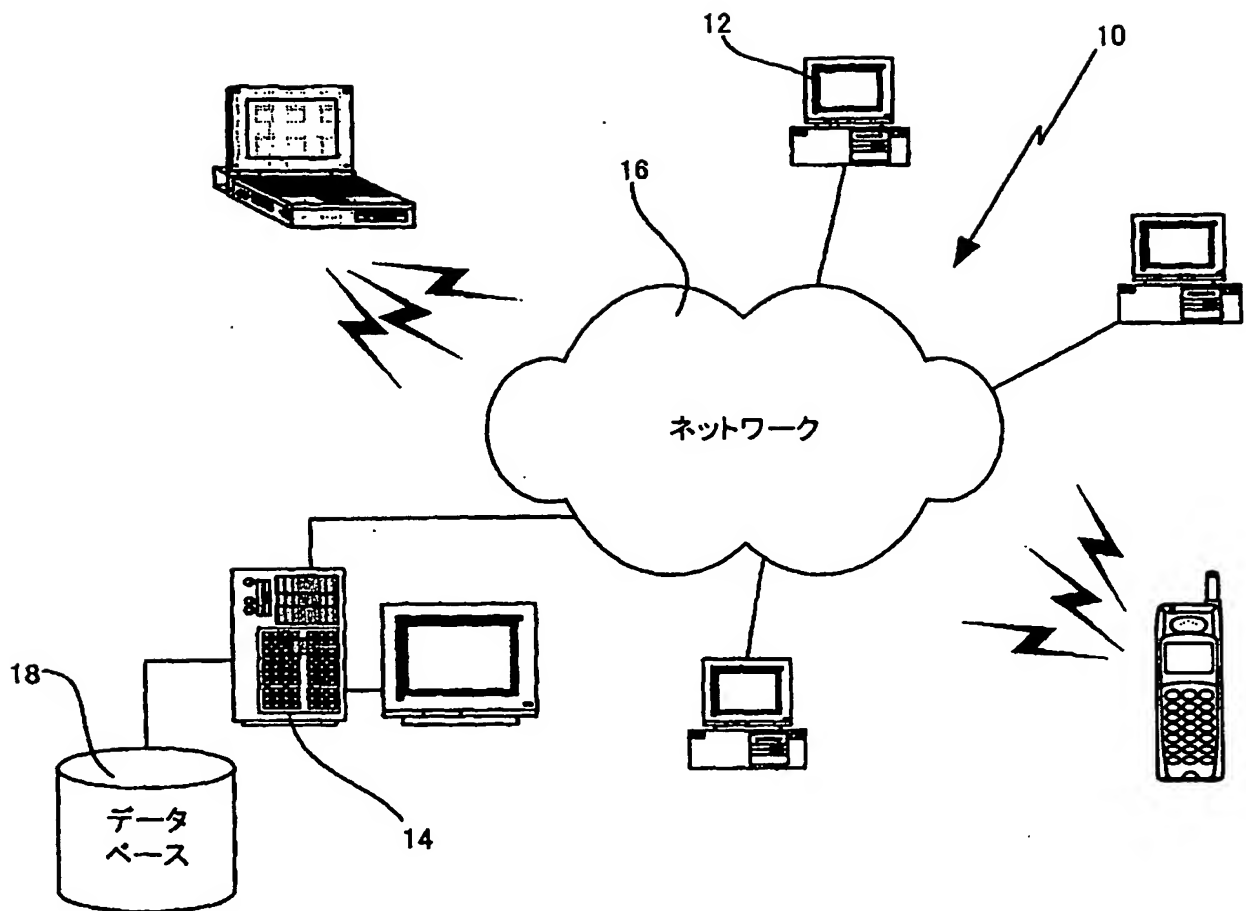
15. コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムは、前記コンピュータ・システムに対して、オブジェクト呼出し要求を受信し格納するステップと、要求オブジェクトへの

- 25 アクセス権限をメモリから取得するステップと、前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、

- 前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記アプリケーションの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索させるステップとを実行させる、プログラム。
- 5 ム。
- 1 6. 前記記憶部が過去に実行された要求オブジェクトの実行結果を格納する場合には、前記検索された実行結果を前記サーバ装置の外部へと送信するステップを実行させる、請求項 1 5 に記載のプログラム。
- 10
- 1 7. 前記記憶部が過去に実行された要求オブジェクトの実行結果を格納しない場合には、前記オブジェクト呼出し要求をオブジェクト実行部へと渡すステップを実行する、請求項 1 5 に記載のプログラム。
- 15 1 8. コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムを記憶したコンピュータ可読な記憶媒体であって、前記プログラムは、前記コンピュータ・システムに対して、オブジェクト呼出し要求を受信し格納
- 20 するステップと、要求オブジェクトへのアクセス権限をメモリから取得するステップと、前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記アプリケーションの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索
- 25 させるステップとを実行させる、コンピュータ可読な記憶媒体。

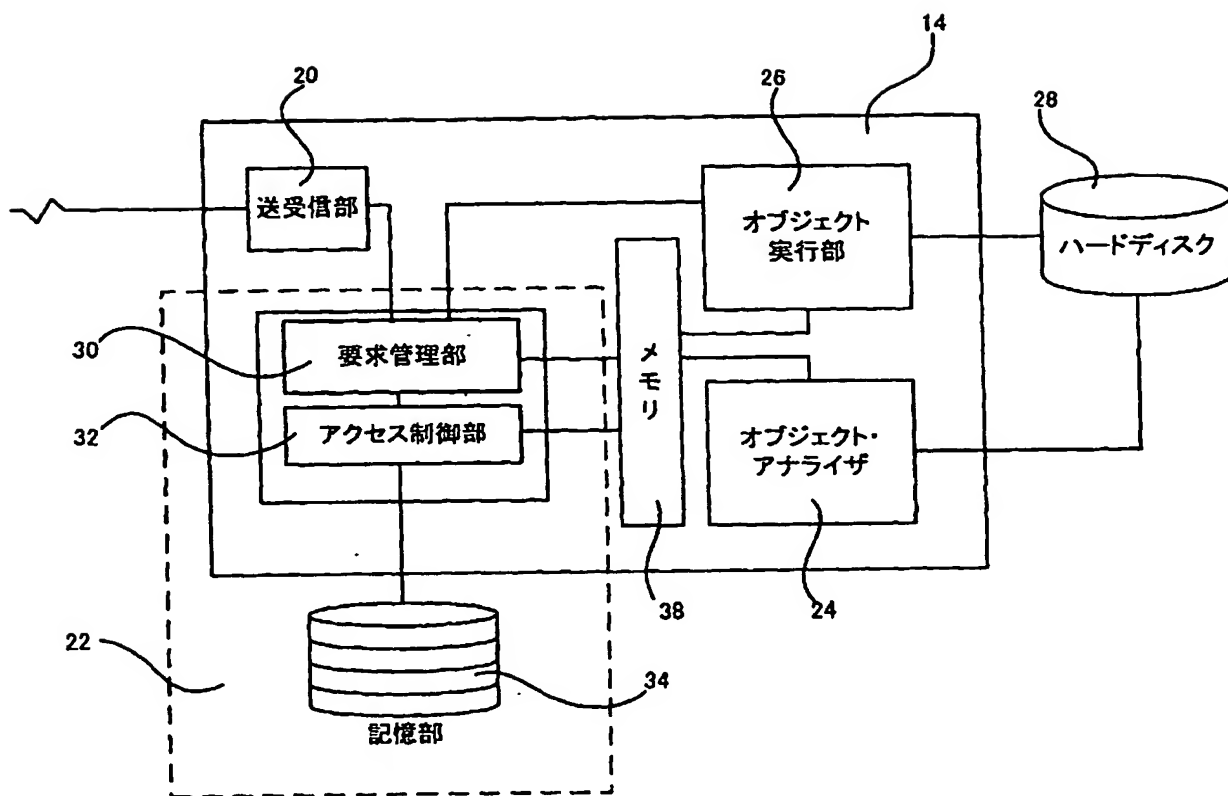
19. コンピュータ・システムをネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムは、前記コンピュータ・システムに対して、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限から生成されるアクセス権限セットをメモリから読出すステップと、前記要求オブジェクトに対する所与のアクセス権限と前記アクセス権限セットとを使用して記憶部に格納されたオブジェクトの過去の実行結果へのアクセスを制御するステップとを実行させるプログラム。
20. コンピュータ・システムをネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムを記憶したコンピュータ可読な記憶媒体であって、前記プログラムは、前記コンピュータ・システムに対して、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限から生成されるアクセス権限セットをメモリから読出すステップと、前記要求オブジェクトに対する所与のアクセス権限と前記アクセス権限セットとを使用して記憶部に格納されたオブジェクトの過去の実行結果へのアクセスを制御するステップとを実行させる記憶媒体。

1/16



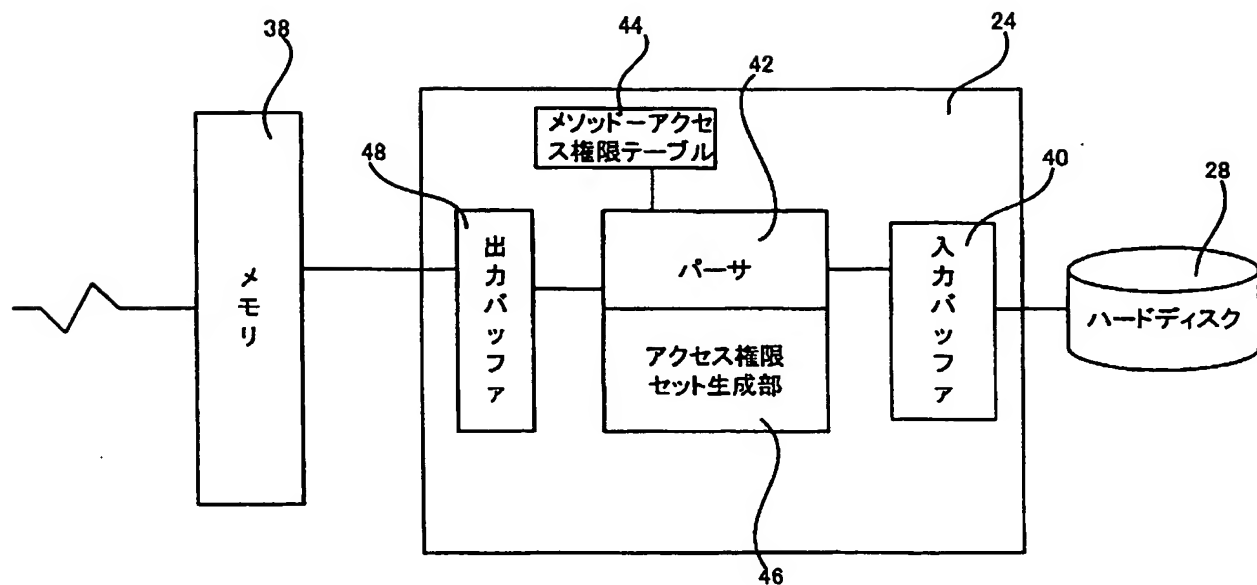
第 1 図

2/16

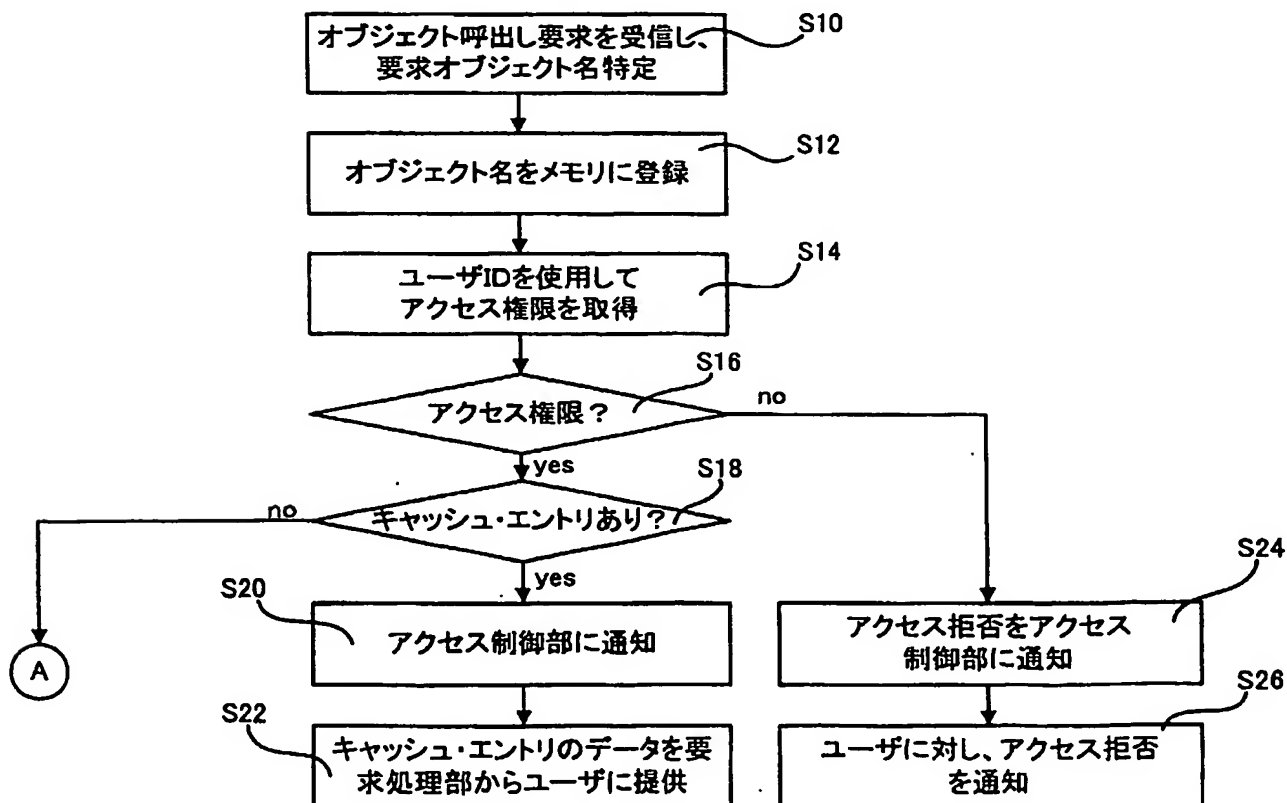


第 2 図

3/16

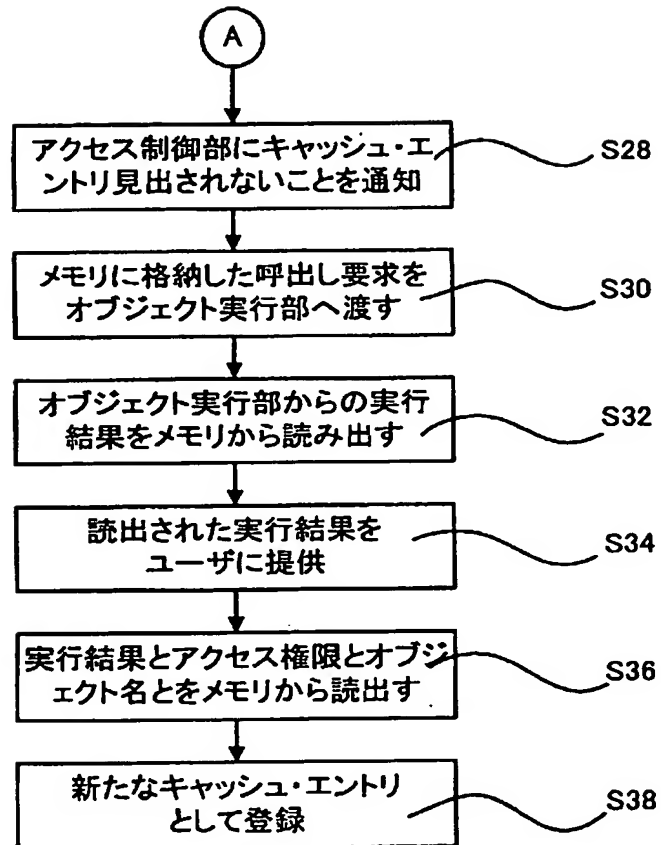


第 3 図



第 4 図

4/16

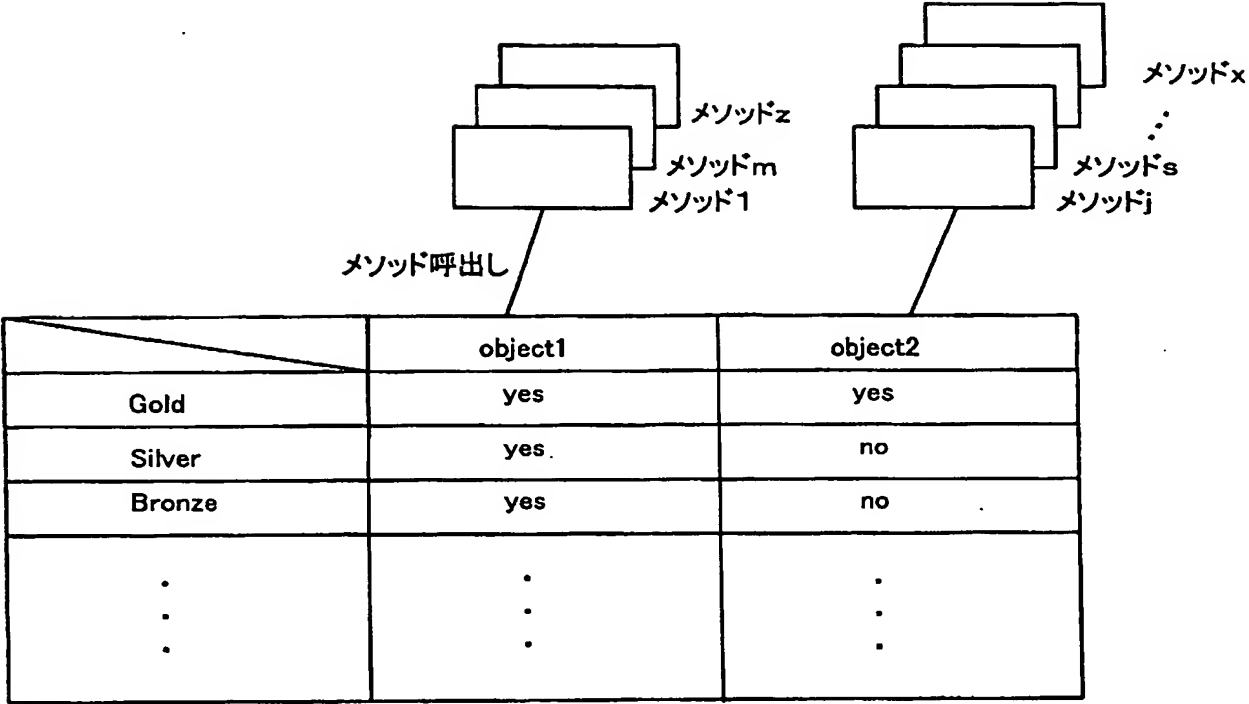


第 5 図

5/16

ユーザID	アクセス権限	
usdxxhnm	gold	A, C, D, ..., X
usboojkn	gold	A, B, M, ..., X
bbioocean	bronz	B, C, M, ..., Y,Z
⋮	⋮	⋮
xjmbiwka	silver	B, J, M, ..., X,Z
lbn123trl	bronz	D, E, F, ..., O,...

第 6 図



第 7 図

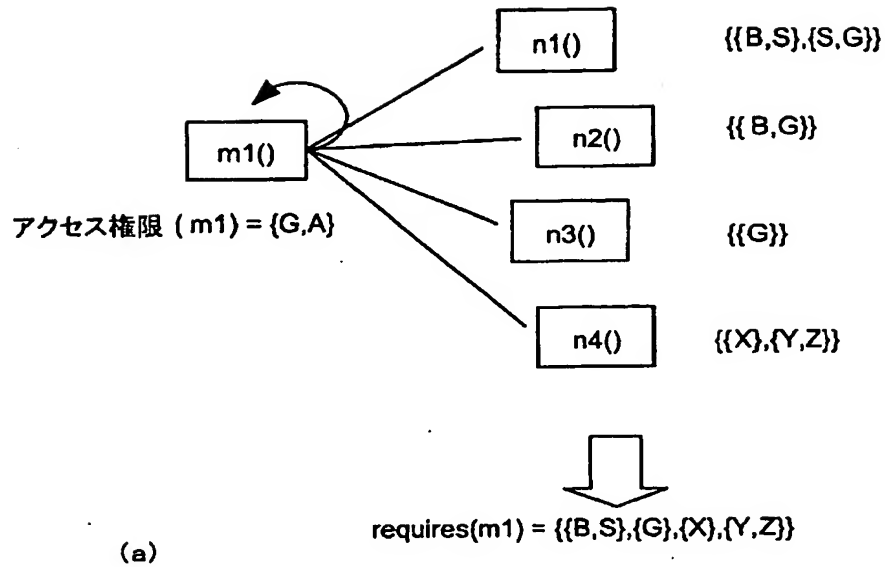
	Method 1	Method 2	...	Method i
Gold	yes	yes		yes
Silver	yes	no		yes
Bronze	no	no		no
A	yes	yes		yes
B	no	yes		no
C	no	no		no
⋮	⋮	⋮		

第 8 図

オブジェクト名	アクセス権限セット	実行結果
getweatherForecast ()	[(G,S),..., (A)]	実行結果1
getweatherForecast ()	[(B), (A)]	実行結果2
getDetailedInfo ()	[(G),..., (X,Y,Z)]	実行結果3
getStockRecommendation ()	[(G,B), (S), ..., (Y)]	実行結果4
getStockRecommendation ()	[(S), (S,B), ..., (Y)]	実行結果5
⋮	⋮	⋮

第 9 図

8/16



$$\begin{aligned}
 \text{requires} (m) &\cong \{ \text{permission} (m) \} \oplus \bigcup_i \text{requires} (n_i) \\
 A \oplus B &\cong \{ r \in A \cup B \mid \neg(\exists s \in A \cup B; r < s) \} \\
 r < s &\Leftrightarrow r \cup s = s \wedge r \neq s \\
 \bigcup_i N_i &\cong N_1 \oplus N_2 \oplus \dots \oplus N_n
 \end{aligned}$$

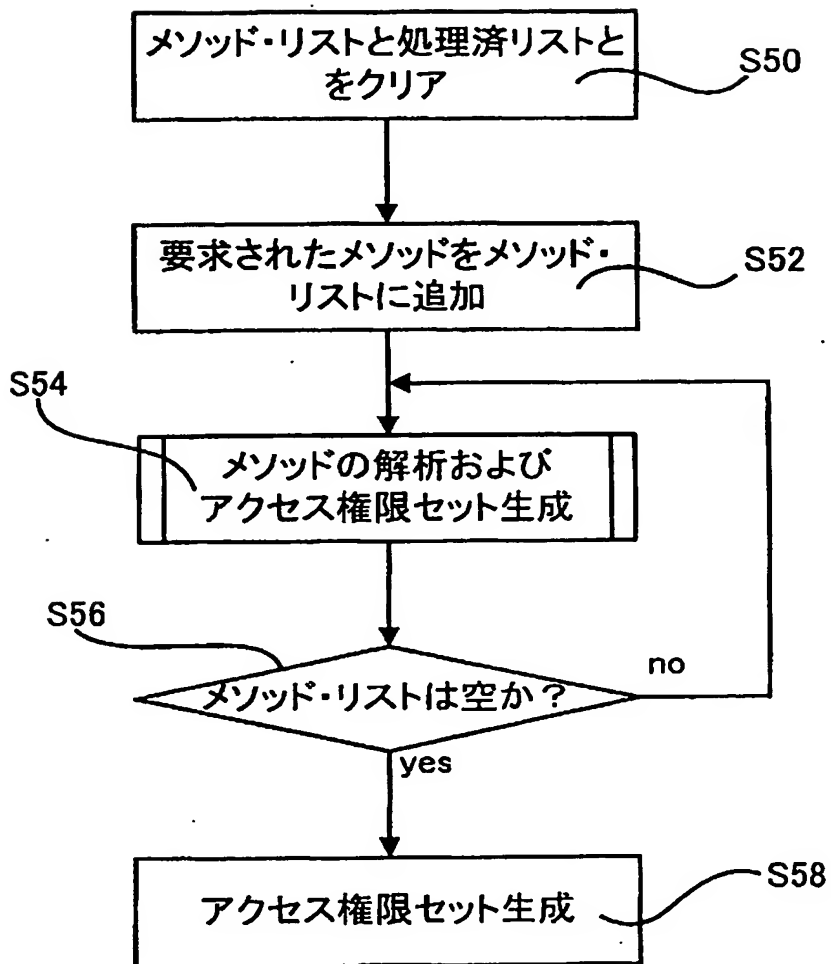
$$\text{unknown} (m) \Rightarrow \text{permission} (m) \cong \emptyset$$

$$\text{safe} (m) \Leftarrow \forall r \in \text{requires} (m); r \cap p \neq \emptyset$$

$p :=$ the roles - set of an accessing principal

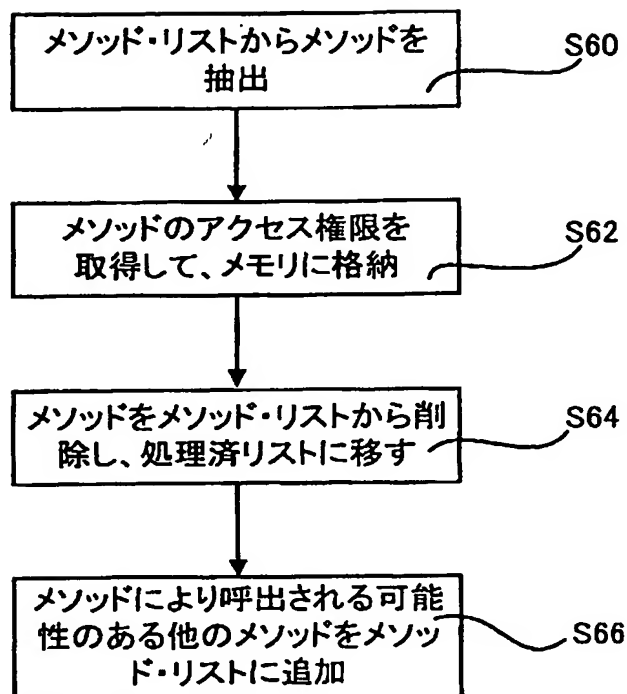
(b)

9/16



第 1 1 図

10/16



第 1 2 図

```

Set<Method> todo-list = {}
Set<Method> done-list = {}
Set<Set<Role>> result = {}

```

```

requiredRoles (method)

```

```

requiredRoles(Method m) {
    Set<Set<Role>> result = {}
    foreach Method n in depends(m) {
        if (n not in done-list) {
            add n to done-list
            add roles allowed for n to result (maybe by taking an optimized form)
            // may optimize result
            requiredRoles(n)
        }
    }
}

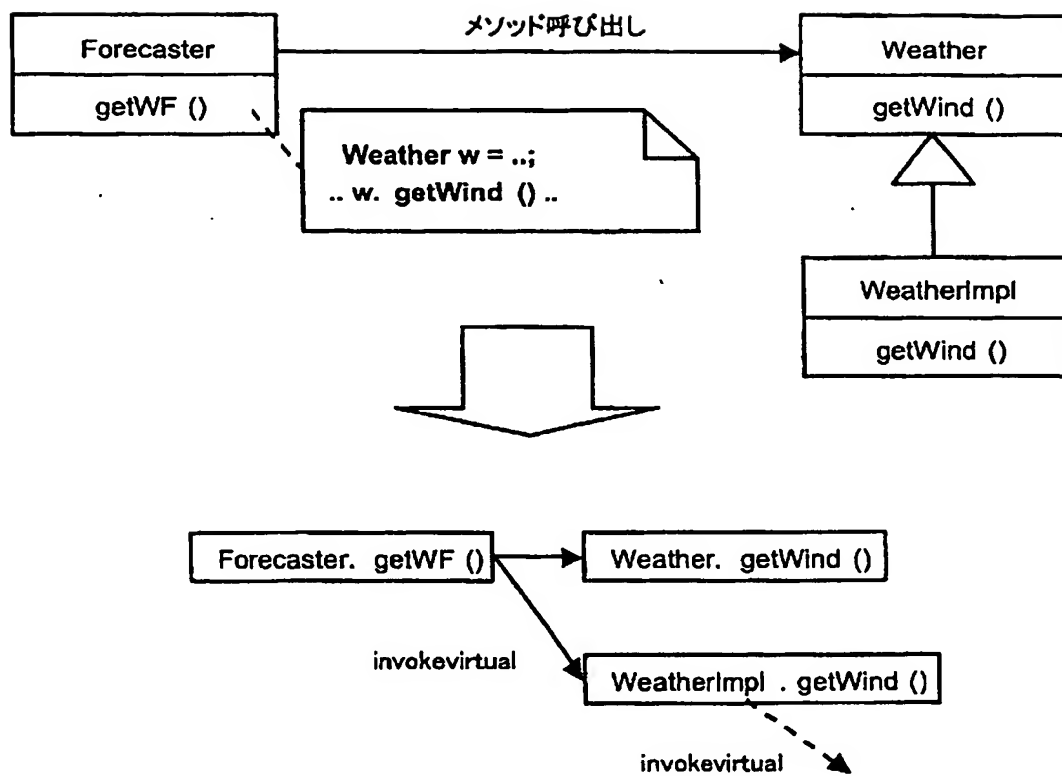
```

Set<Set<Role>> represents a set of a set of Role sets.

The depends() returns all of methods that may be directly invoked from the given method.

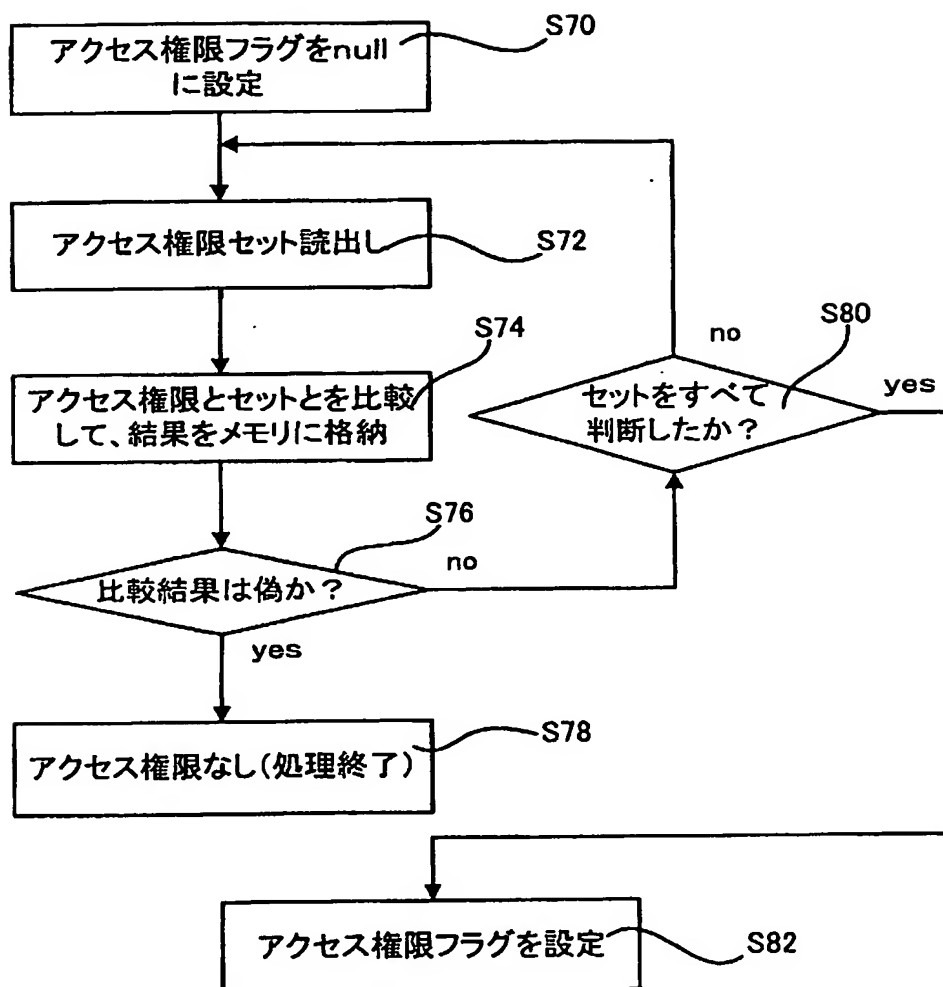
第 1 3 図

11/16



第 1 4 図

12/16



第 1 5 図

13/16

```

Principal p
Set<Set<Role>> roleCondition = { (A, B), (B, C), (X, Y, Z) }

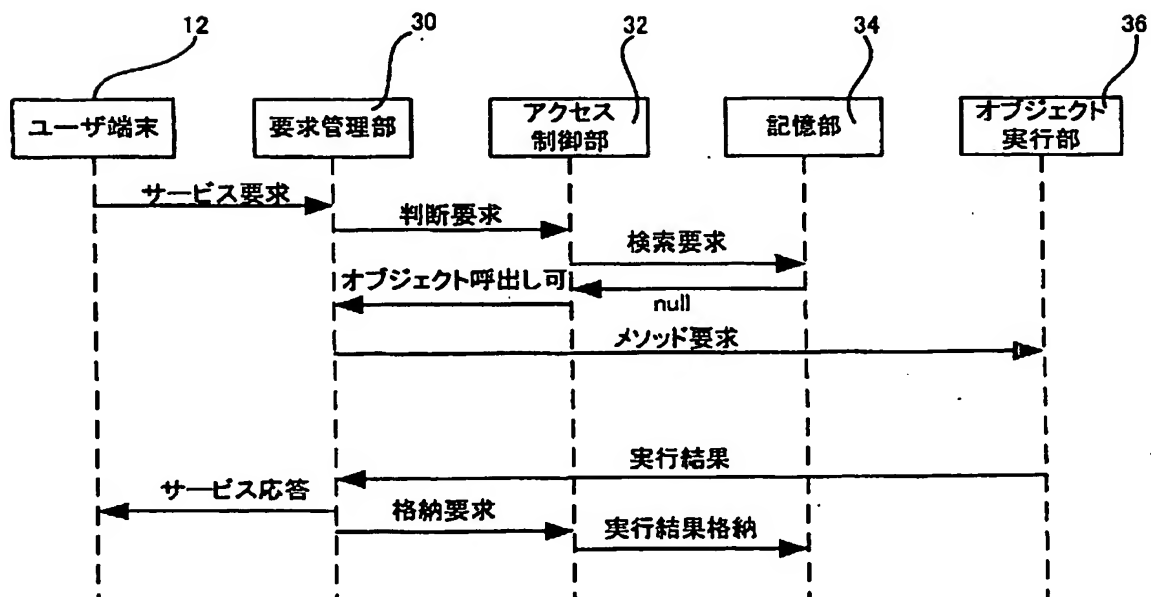
if compliesWith(roleCondition) then success else failure

boolean compliesWith(Set<Set<Role>> roleCondition) {
    foreach Set<Role> allowedRoles in roleCondition {
        if not isInAnyOf(allowedRoles) return false
    }
    return true
}

boolean isInAnyOf(Set<Role> allowedRoles) {
    foreach Role role in allowedRoles {
        if p in role then return true
    }
    return false
}

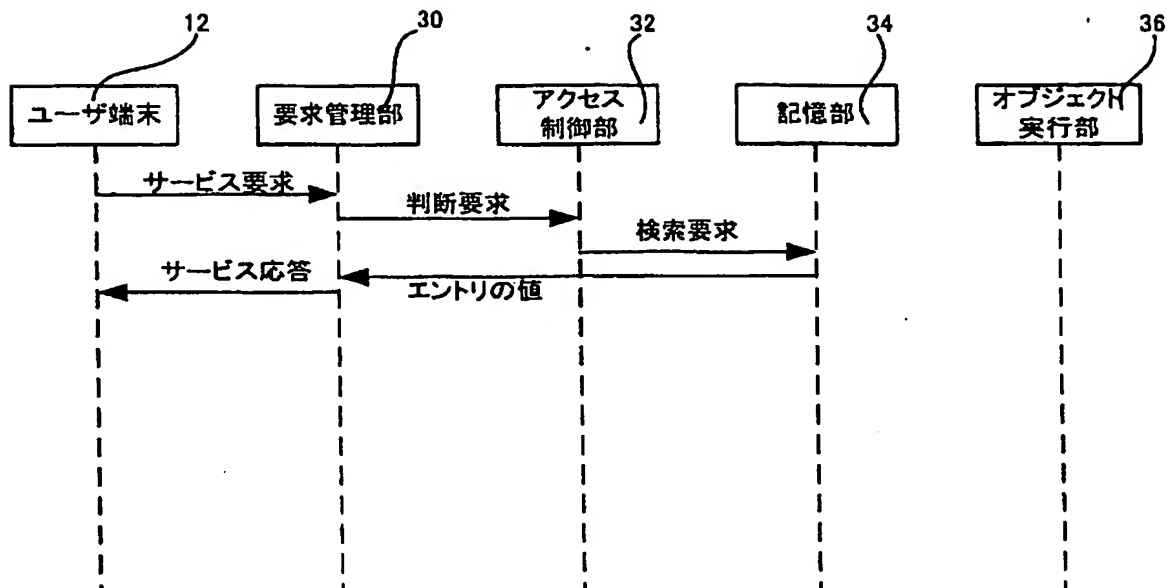
```

第 1 6 図

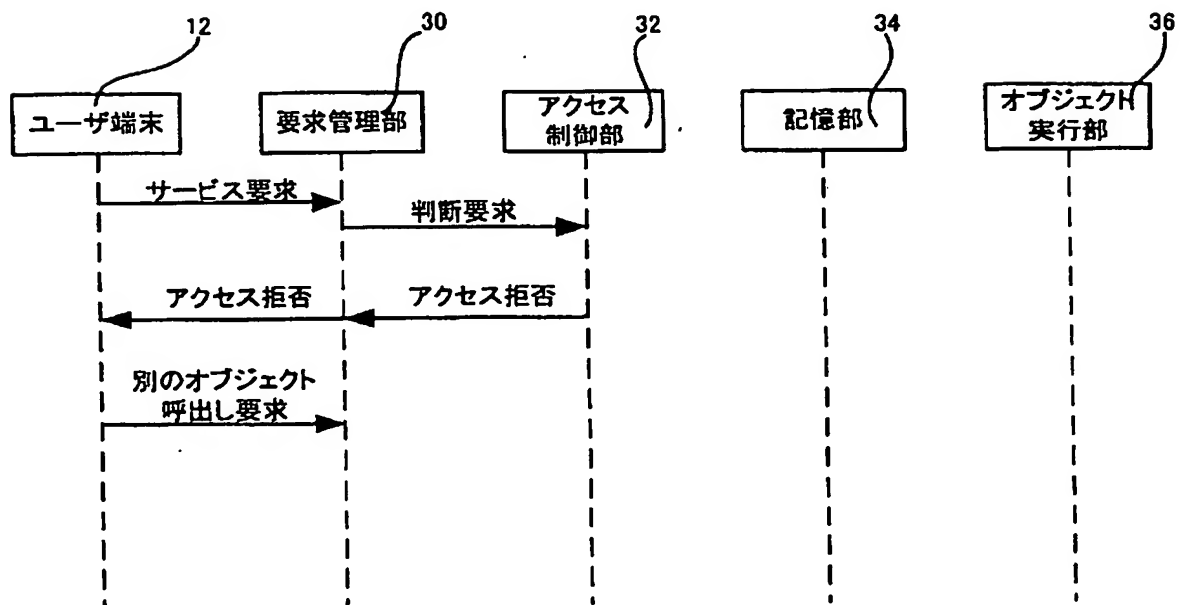


第 1 7 図

14/16

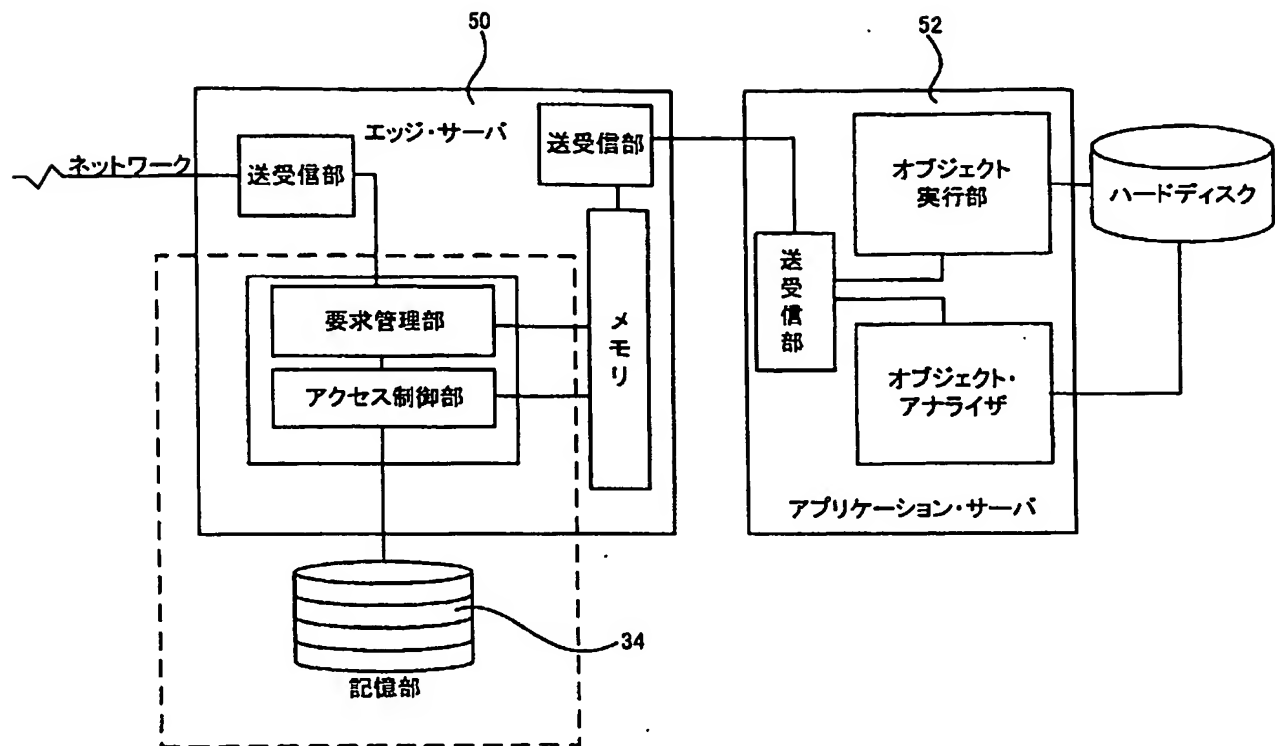


第 1 8 図

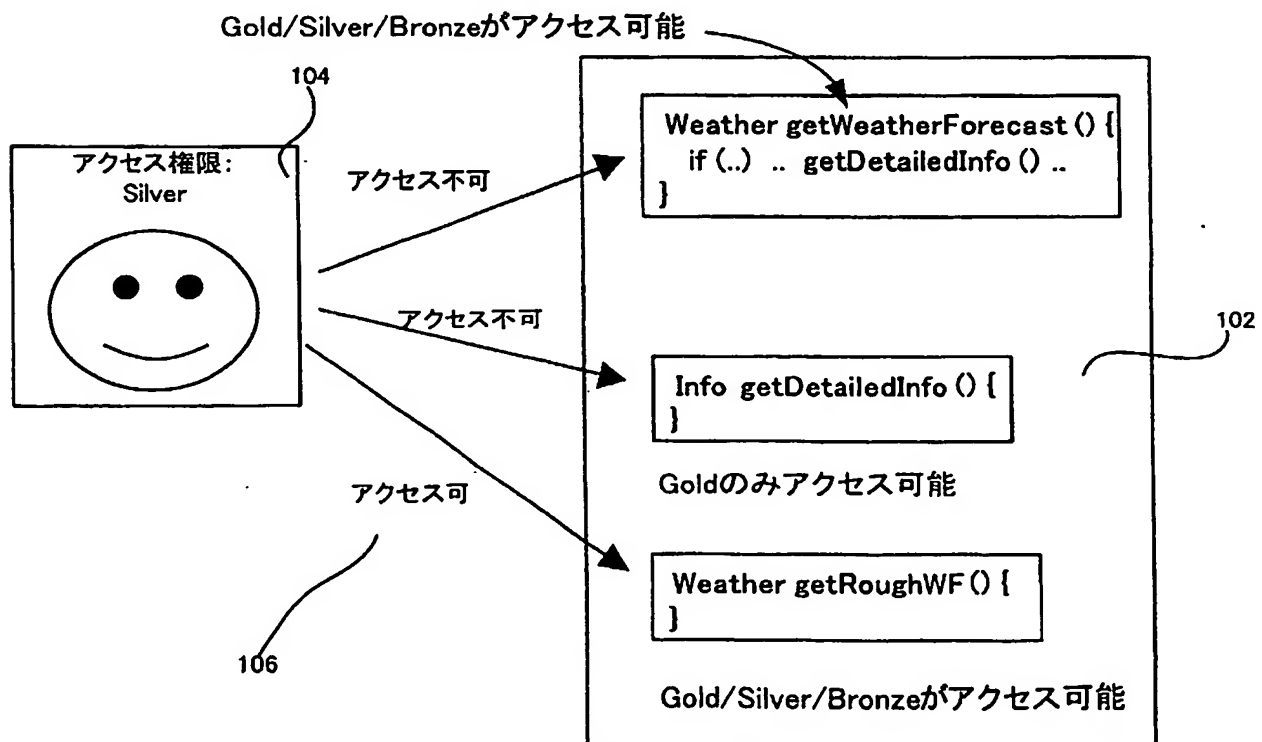


第 1 9 図

15/16

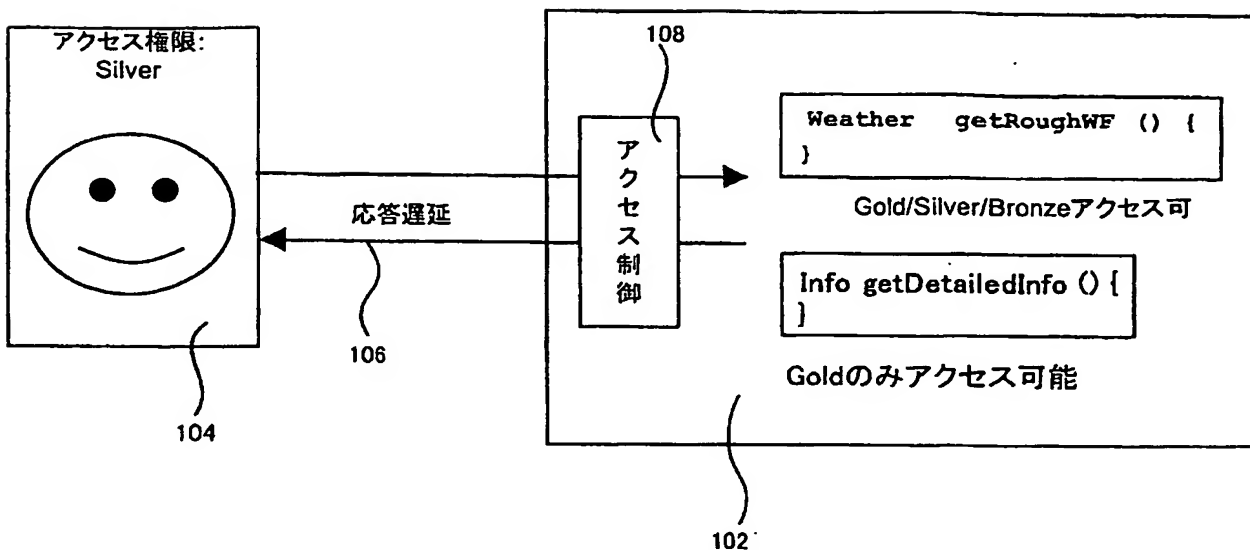


第 20 図

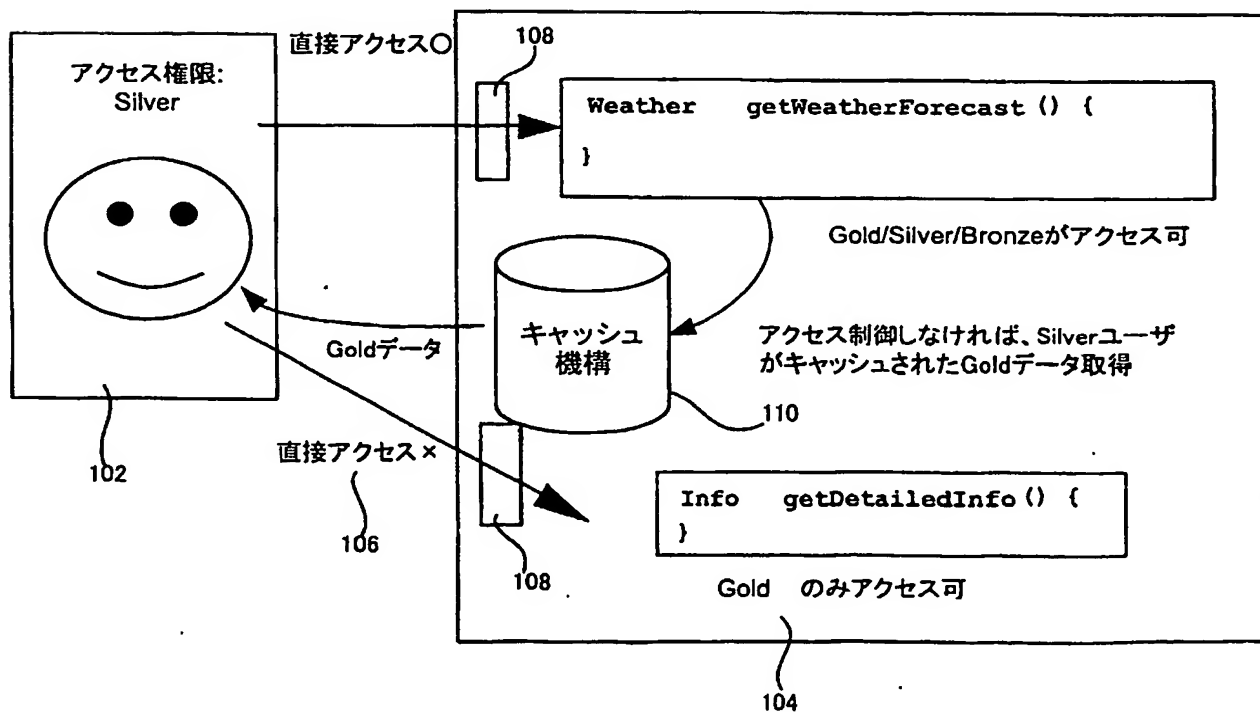


第 21 図

16/16



第 2 2 図



第 2 3 図

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/16130

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F15/00, G06F12/00, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F15/00, G06F12/00, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-120048 A (Fujitsu Ltd.), 30 April, 1999 (30.04.99), Full text; Figs. 1 to 7 & GB 9805825 A & US 6243719 B	1-20
A	JP 11-175475 A (Nippon Telegraph And Telephone Corp.), 02 July, 1999 (02.07.99), Full text; Figs. 1 to 5 (Family: none)	1-20
A	JP 2001-167032 A (International Business Machines Corp.), 22 June, 2001 (22.06.01), Full text; Figs. 1 to 14 & CN 1305145 A & US 2001-16872 A	1-20

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
21 January, 2004 (21.01.04)

Date of mailing of the international search report
03 February, 2004 (03.02.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, G06F12/00, G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, G06F12/00, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2004年
日本国登録実用新案公報 1994-2004年
日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-120048 A (富士通株式会社) 1999. 04. 30, 全文, 第1-7図 & GB 9805825 A & US 6243719 B	1-20
A	JP 11-175475 A (日本電信電話株式会社) 1999. 07. 02, 全文, 第1-5図 (ファミリーなし)	1-20

☒ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技术水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

21. 01. 2004

国際調査報告の発送日

03. 2. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

後藤 和茂

5 B

9 4 6 3

電話番号 03-3581-1101 内線 6907

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2001-167032 A (インターナショナル・ビジネス・マシーンス・コーポレーション) 2001. 06. 22, 全文, 第1-14図 & CN 1305145 A & US 2001-16872 A	1-20